LIBRO BLANCO

UNA INICIATIVA CATALANA PARA LA SEGURIDAD EN LAS TIC

Una iniciativa catalana para la seguridad en las TIC

Fruto de una reflexión con diferentes expertos en seguridad, este capítulo presenta un conjunto de áreas de actuación que podrían formar parte de una iniciativa catalana para la seguridad en las TIC.

En algunas de estas áreas de actuación ya hay organismos, públicos o privados, trabajando de forma parcial pero a partir de su estudio detallado se ha llegado a la conclusión de que estas iniciativas no buscan una respuesta global como país y de que casi en todos los casos son iniciativas aisladas, es decir, sin relación entre ellas.

1_PRINCIPIOS

Los principios que nos mueven en la propuesta de creación de una iniciativa catalana de seguridad en las TIC son los siguientes:

1. La seguridad en las TIC tiene un ámbito general, por lo cual, si sólo se plantea desde una visión sectorial (sector público, sector de la construcción, sector de la distribución, etc.), la seguridad final es el punto más débil de los diferentes sectores en el momento en que se interconectan. Esto no era un problema hasta ahora, pues eran sectores cerrados, pero en el momento en que aparece Internet y las relaciones que se establecen en el ámbito intersectorial ya requieren niveles de seguridad, la problemática aparece de forma muy importante.
2. Esta visión ya se está teniendo en cuenta desde diferentes estados en el ámbito europeo e incluso en el ámbito de fuera de Europa. Solamente es necesario ver documentos como los siguientes:
   a) «Retos para la sociedad de la información europea más allá de 2005», COM (2004) 757, de 19 de noviembre de 2004, y
   b) «i2010. Una sociedad de la información europea para el crecimiento y el empleo», COM (2005) 229, de 1 de junio de 2005,

los cuales ya hablan de esta necesidad, pero muy especialmente el documento «Una estrategia para una sociedad de la información segura – Diálogo, asociación y potenciación», COM (2006) 251, de 31 de mayo de 2006.

3. Pensamos que, con el conocimiento existente hoy en día en el ámbito de Cataluña, con las iniciativas que hoy son una realidad en este campo y con el liderazgo que en algunos sectores hay respecto a esta materia, Cataluña puede convertirse en un referente en estos aspectos y promover internamente esta cultura de seguridad en las TIC.

4. Si Cataluña tiene este nivel de seguridad, las negociaciones en relación con otras comunidades se establecerán bajo el nivel de seguridad propio y no sobre posibles futuros niveles de seguridad que se puedan estandarizar; es decir, si pudiésemos decir en un futuro que Cataluña tiene un nivel de seguridad 5, podríamos condicionar que las relaciones establecidas con Cataluña deberían tener como mínimo este nivel de seguridad.

5. Estos conocimientos, que diferentes personas y entidades catalanas tienen sobre los distintos aspectos de la seguridad en las TIC, podemos agruparlos dentro de esta iniciativa y hacer que Cataluña se convierta en un referente en estos aspectos, con la posibilidad de que desde fuera traigan inversiones al respecto, y que no nos pase como en la compra de Netfocus por parte de HP, que finalmente no ha servido para traer a Cataluña el centro mundial de HP con relación a la identidad digital.

6. Es necesario que esta iniciativa cuente con la participación tanto del sector público, que la debe liderar, como del sector privado, y muy especialmente de la sociedad civil catalana, que en Cataluña tiene una clara tradición en el fomento e impulso de este tipo de iniciativas.

2_ÁREAS ESTRATÉGICAS

Planteamos esta iniciativa catalana para la seguridad en las TIC desde el desarrollo de 8 áreas estratégicas, con unos contenidos propios pero a la vez relacionadas entre ellas:

Área 1: Establecimiento de una estrategia global de seguridad de la información

Como tarea más importante dentro de esta área, se debe proceder al desarrollo de una estrategia global de seguridad de la información en el ámbito catalán, que esté coordinada con las posibles estrategias nacionales o internacionales que eventualmente se puedan producir y que las complemente.

Esta estrategia debe estar liderada desde el sector público, y abarcar tanto al sector público como al privado y a la sociedad civil catalana, de forma coordinada con las políticas de administración electrónica y de impulso de la sociedad de la información y el conocimiento.

Así mismo, debe considerar de forma global las necesidades de seguridad civil en el uso de las redes de la información mediante una aproximación amplia, que tome en consideración los aspectos técnicos, socioeconómicos y legales, cosa que implica una dimensión multidisciplinar de las políticas.

Algunos de los instrumentos a utilizar para la implementación de esta estrategia de seguridad incluyen las asociaciones público-privadas, el desarrollo de mejores prácticas, el suministro de consejo y la participación en órganos comunes.

En cuanto al gobierno de la iniciativa de seguridad, es necesario situarlo al más alto nivel, de forma que resulte efectivo, tanto dentro de Cataluña como en las relaciones con el Estado y los organismos internacionales.

Área 2: Impulso de la concienciación y formación respecto a la seguridad de la información

En segundo lugar, resulta necesario conseguir incrementar los niveles de conciencia respecto a la necesidad de la seguridad de la información, a la cual la OCDE denomina la «cultura de la seguridad». Los gobiernos deben desarrollar políticas públicas nacionales o regionales sobre seguridad de la información y garantizar la cooperación internacional para promover esta cultura global de la seguridad mediante instrumentos como los siguientes:

- Medidas legales y técnicas para combatir la ciberdelincuencia, consistentes con la Convención del Consejo de Europa.

- Equipos y recursos personales altamente cualificados para ayudar a la lucha coordinada contra el fraude informático.
- Instituciones preparadas para responder a ataques y a emergencias informáticas, así como para intercambiar información al respecto, como por ejemplo los denominados CERT.
- Mecanismos de cooperación con el sector privado para combatir con mayor efectividad los problemas de seguridad.
- Apoyo a la investigación y el desarrollo en el campo de la seguridad de las tecnologías de la información.
- Actividades de concienciación pública, de formación y de educación del público.
- Suministro de recursos de información al público sobre la seguridad de los sistemas y de las redes de información.

Área 3: Fomento de la protección de la seguridad de las infraestructuras críticas de información y comunicaciones

La tercera área estratégica se refiere a la protección de las infraestructuras críticas, que ha recibido una atención particular a raíz de los ataques terroristas de los últimos años.

Las infraestructuras críticas son instalaciones, redes, servicios y equipamientos físicos y de tecnología de la información cuya interrupción o destrucción tendría un impacto mayor en la salud, la seguridad o el bienestar económico de los ciudadanos, o en un funcionamiento eficaz de los gobiernos de los estados miembros. Las infraestructuras críticas se encuentran presentes en numerosos sectores de la economía: actividades bancarias y financieras, transporte y distribución, energía, servicios, salud, suministro de alimentos, comunicaciones, administraciones públicas clave…

Las consecuencias de un ataque contra los sistemas industriales de control de las infraestructuras críticas podrían ser muy variadas. Se considera que un ataque cibernético causaría pocas víctimas o ninguna, pero podría implicar la pérdida de servicios de infraestructura vitales, como por ejemplo el servicio telefónico de los servicios de emergencia, mientras que ataques contra los sistemas de control de infraestructuras químicas podrían implicar escapes de materiales tóxicos, que en este caso podrían producir víctimas mortales.

El sector público, que frecuentemente es propietario o regulador de estas infraestructuras, debe asumir un papel de liderazgo en la protección de las infraestructuras críticas en Cataluña, de forma conectada con el resto de políticas públicas en seguridad de la información.

Área 4: Establecimiento de una red catalana de centros de respuesta a incidentes de seguridad

Los centros de respuesta a incidentes de seguridad facilitan el hecho de compartir la información de seguridad dentro de un grupo de miembros que operan en sectores similares, con una fuerte orientación a la cooperación internacional, lo que permite un mejor intercambio de información y buenas prácticas.

Entre otras tareas, se encargan del seguimiento y detección de problemas de seguridad, incluyendo virus informáticos, y preparan y, más corrientemente, divulgan la información necesaria para minimizar los posibles daños derivados.

Una red catalana de centros de respuesta a incidentes de seguridad, liderada desde el sector público y coordinada con redes nacionales e internacionales ayudará significativamente a la mitigación de los riesgos de seguridad, en especial de las entidades públicas y privadas que menos recursos tecnológicos especializados pueden disponer, como las PYME o los ayuntamientos de dimensión reducida.

Área 5: Colaboración en la lucha contra las comunicaciones comerciales no solicitadas (SPAM) y contra la pesca pirata *(phishing)*

El SPAM se ha incrementado de forma muy significativa durante los últimos cinco años, y supone entre el 50% y el 80% de todos los mensajes de correo electrónico que reciben los usuarios, con un coste superior a los 39.000 millones de euros en 2005.

El SPAM ha pasado de ser una práctica comercial, molesta para algunos pero esencialmente lícita, a ser cada vez más un instrumento de fraude y comisión de delitos, como es el caso de los mensajes de pesca pirata (*phishing*), en los que se suplanta la identidad de páginas web lícitas, como las páginas de las entidades financieras, con la intención de robar la identidad (y la contraseña) de los usuarios o perjudicar la reputación de dichas entidades.

Por otro lado, se continúa incrementando el uso del correo electrónico para la diseminación de software espía o de software de captura del comportamiento en línea de los usuarios. En muchos casos, este software espía puede obtener información personal confidencial y divulgarla, como ocurre con los números de tarjetas financieras y otras informaciones personales.

Es necesario que, tanto el sector público como el privado y también la sociedad civil se involucren de forma activa en la lucha contra estos fenómenos, el SPAM y el *phishing*, y sus futuras formas de proliferación, en colaboración con el resto de agentes que trabajan en ella.

Área 6: Seguridad dentro de la administración electrónica

Una de las fórmulas importantes para conseguir incrementar el nivel global de seguridad es la actuación de los estados y, en concreto, la incorporación de la seguridad al procedimiento administrativo electrónico, debido al impacto directo e indirecto sobre la sociedad en su conjunto, indudablemente relacionado con el volumen del sector público en la economía.

Es necesario continuar fomentando las siguientes iniciativas:

- Vigilancia, alerta y respuesta a incidentes de seguridad en las AA. PP.
- Cumplimiento por parte de las AA. PP. de los estándares, recomendaciones o manuales de seguridad, especialmente aquellos establecidos a partir de la norma ISO 17799.
- Desarrollo de las infraestructuras de clave pública (PKI) para la comunicación con y entre las AA. PP., tarea que ya está siendo realizada desde CATCert.
- Desarrollo de software por parte de las AA. PP., como por ejemplo aplicaciones de administración electrónica que hagan uso de la tarjeta de ciudadano, servicios de correo electrónico seguro o intercambio seguro de informaciones por redes inseguras, con y sin hilos. En este sentido, también se deben mencionar iniciativas de CATCert, como el Validador, PASSI o iArxiu.
- Servicios de pruebas de intrusión para las AA. PP.
- Servicios de consultoría y formación a las AA. PP.
- Desarrollo de redes seguras de comunicaciones por servicios, por ejemplo, de emergencia. En este sentido, se puede mencionar la

tarea de aseguramiento de las redes de intercambio de documentos entre administraciones públicas, especialmente en el caso de la red del Consorcio AOC.

- Servicios centralizados de copia de seguridad para sistemas de información operados por AA. PP.
- Implantación de proyectos de cooperación para dar a conocer la cultura de la seguridad entre las AA. PP.
- Medida de la eficiencia de las políticas de seguridad y de su implementación a partir de la realización de auditorías.

En particular, se debe incidir en que las infraestructuras necesarias para la prestación de servicios electrónicos y para el apoyo de la administración electrónica deben estar bajo control del gobierno, con independencia de la modalidad de gestión directa o indirecta de la misma, evaluando los riesgos que supone para la continuidad de las operaciones del sector público que servicios críticos como la validación electrónica del DNI electrónico y otros certificados se sustente en servicios prestados fuera de Cataluña (por ejemplo, por organismos como el MAP o la FNMT-RCM).

Área 7: Colaboración y apoyo en la lucha contra la ciberdelincuencia

La sociedad de la información supone oportunidades indudables de desarrollo humano, social y económico, pero su estructuración permite también la aparición de nuevas formas de criminalidad usando la tecnología. Además, las consecuencias de los comportamientos delictivos pueden tener efectos de alcance superior dada la ausencia de limitaciones geográficas o fronteras nacionales, como demuestran los ataques a la propiedad intelectual o los virus informáticos; mientras que, por otro lado, las medidas técnicas de protección de los sistemas de información deben implementarse siguiendo las medidas legales de prevención y lucha contra los delitos y de acuerdo con ellas.

Con relación a la lucha contra el crimen electrónico, resulta necesario ofrecer apoyo a las policías y otras fuerzas de seguridad, así como ayudar a proteger los sistemas de modo que se reduzcan estas conductas, por ejemplo mediante sistemas de evidencia electrónica más eficaces.

Área 8: Fomento de la investigación y desarrollo en seguridad de la información

La investigación y desarrollo en materia de seguridad de la información es una de las políticas más habituales de los estados avanzados en la cultura de la seguridad, especialmente por el impacto posterior en la competitividad de las empresas productoras de tecnologías de seguridad, que comercializan sus productos en el mercado global.

En este sentido, desde una perspectiva de política de la Unión Europea, la Resolución del Consejo de 22 de marzo de 2007, sobre una estrategia para una sociedad de la información segura en Europa, considera que los recursos destinados a investigación y desarrollo (I+D) e innovación, tanto en el ámbito nacional como comunitario, constituyen uno de los elementos fundamentales para reforzar el nivel de seguridad de las redes y de la información de los nuevos sistemas, aplicaciones y servicios.

Cataluña no puede quedar fuera de esta oportunidad, sino que debe participar de ella activamente, impulsando la creación de tecnología propia de seguridad de la información y promocionándola por todo el mundo.

Para alcanzar este objetivo, puede resultar beneficioso que desde el sector público se concentren los esfuerzos de canalización de proyectos nacionales e internacionales en el tejido empresarial de Cataluña, mostrando especial atención al sector del software libre.

3_MODELO PROPUESTO

Para llevar a cabo estas iniciativas, pensamos que lo mejor sería crear un consorcio, una fundación o algún otro instrumento jurídico, participado por el sector público y la sociedad civil catalana, con la colaboración del sector privado. Este modelo es el que está funcionando en otras comunidades autónomas y en otros ámbitos, en otros países europeos y de fuera de Europa.

Desde este libro queremos proponer como integrantes indispensables a la Generalitat de Cataluña, a Localret y a las Cámaras de Comercio.

LIBRO BLANCO

LISTA DE CONTROL. UN CAMINO HACIA ADELANTE (ICC)

Lista de control de la seguridad. Un camino hacia delante (ICC)

1_USO DE LOS PRINCIPIOS

Esta sección sigue las Directrices de la OCDE, pero reajusta sus principios para potenciar las consideraciones prácticas, la toma de decisiones e implementación presentes en las buenas prácticas de seguridad. Las palabras o frases entre paréntesis se refieren al principio de las Directrices de la OCDE. Esta guía se centra en dos únicas categorías: qué debería usted saber, y qué tiene usted que hacer.

Qué debería usted saber

- ¿Qué necesito saber sobre la seguridad de la información en mi empresa? (Conocimiento).
- ¿Cómo puedo entender las amenazas, vulnerabilidades, y efectos sobre mis sistemas, procesos y empleados? (Evaluación de riesgo).
- ¿Qué se espera de mí teniendo en cuenta el tamaño y la naturaleza de mi empresa? (Responsabilidad).
- ¿Qué obligaciones sociales tengo que conocer? (Ética y Democracia).

Qué tiene usted que hacer

- Crear e implementar una política de seguridad (Diseño e implementación de la seguridad).
- Factores que se han de considerar a la hora de seleccionar e implementar soluciones (Diseño e implementación de la seguridad).
- Desarrollar e implementar prácticas y procedimientos (Gestión de la seguridad / Conocimiento).
- Como gestionar los incidentes (Respuesta).
- Revisar y mejorar los procesos y sistemas (Nuevas evaluaciones).

Esta guía se compone básicamente de listas de control y de posibles soluciones. Como la seguridad no es algo que tenga solo una posible solución, se tienen que determinar los requisitos basándose en las necesidades de su negocio, el tipo de información que se maneja y la naturaleza de sus infraestructuras técnicas.

Qué debería usted saber

A continuación hay una serie de listas de comprobación que le ayudarán a calcular las necesidades de seguridad de la información de su empresa.

Entender la importancia de la información en su empresa (Conocimiento)

- ¿En qué medida está relacionada la información que usted maneja con la consecución de sus objetivos primarios?
- ¿Ha identificado usted la información que es crucial para su empresa?
- ¿Qué actividades se hacen en su empresa que supongan la creación, el procesamiento, almacenamiento, uso y transmisión de la información crucial para la empresa?
- ¿Qué activos usa para crear, procesar, almacenar y transmitir dicha información crucial para la empresa (por ejemplo ordenadores, ficheros, teléfonos móviles)?
- ¿Sabe lo que le ocurriría a su empresa si resultase comprometida la confidencialidad de dichos activos (es decir, si la competencia tuviera acceso a ellos)?
- ¿Sabe lo que le ocurriría a su empresa si resultase comprometida la integridad de dichos activos, y no pudiese confiar en la información que contienen?
- ¿Sabe lo que le ocurriría a su empresa si usted no pudiese disponer de dichos activos durante una hora, un día, una semana, o un mes?
- ¿Usando lo que ahora conoce sobre la confidencialidad, integridad y disponibilidad de los activos que contienen la información en su empresa, puede priorizarlos?

Una vez haya priorizado los activos de la información según su importancia en la empresa, usted estará seguro de que se les da el grado de protec-

ción apropiado. No hacerlo podría suponer perder tiempo y recursos en activos que no son cruciales para su empresa; o peor, que la información crucial para la empresa no está adecuadamente protegida.

Conocer los activos relacionados con la seguridad de la información (Evaluación de riesgo)

- ¿Ha hecho un inventario de los activos que contienen información crucial para la empresa: hardware, software y propiedad intelectual (como patentes y contratos)?
- ¿Indica el inventario dónde se pueden encontrar dichos activos?
- ¿Se actualiza regularmente el inventario y se audita para asegurarse de que es exhaustivo y válido?
- ¿Está al corriente de las características de seguridad de su hardware y su software, y tiene los manuales pertinentes o material de apoyo de esas características?
- ¿Tiene alguien de la empresa experiencia previa en estos productos o ha hecho un cursillo para aprender su funcionamiento?

Conocer cómo se utilizan los activos, quién los utiliza y por qué razón (Conocimiento)

- ¿Quién en su empresa tiene acceso a los activos cruciales para la empresa?
- ¿Usan sus empleados contraseñas únicas para controlar el acceso a los ordenadores que usan?
- ¿Se mantienen en lugar seguro y cambian regularmente dichas contraseñas?
- ¿Se asegura de que las contraseñas se dan únicamente si es necesario por cuestiones laborales?
- ¿Tiene listas de quién tiene acceso y se renuevan periódicamente estas listas?
- ¿Tiene una red local o mayor? Si la tiene, ¿cómo controla el acceso a la red? Si se usan contraseñas, ¿son únicas para cada usuario, se cambian regularmente y guardan en un lugar seguro?
- ¿Tiene acceso a Internet? Si lo tiene, ¿tiene acceso de banda ancha o marcación?

- ¿Qué ordenadores / aparatos de la empresa tienen red o acceso a Internet?, y ¿tiene conocimiento de quién los usa?
- ¿Tienen los empleados acceso remoto a su red (ya sea desde casa o desde la calle)?
- ¿Cómo acceden a la red sus empleados cuando están trabajando fuera de la empresa?

Conocer la gestión de la seguridad (Conocimiento)

- Lea la siguiente lista de tecnología para la seguridad y pregúntese cuáles conoce y cuáles usa:
  - firewalls y RPV (Red Privada Virtual)
  - controles de acceso, autorización y autentificación
  - antivirus
  - filtros de spam
  - parches del software
  - control de conexión a Internet
  - herramientas para las políticas de seguridad de las redes
  - bases de datos de vulnerabilidades y amenazas
  - herramientas de criptografía como el SSL, criptografía de claves públicas y encriptación del disco duro
  - sistemas de detección de intrusos
- ¿Hace regularmente copias de seguridad de su información crucial?
- ¿Hace pruebas de las copias de seguridad, y realmacena la información para asegurarse que sigue siendo utilizable?
- ¿Se sacan de la empresa copias de seguridad con regularidad?
- ¿Suele arreglar cualquier vulnerabilidad de los softwares que utiliza en la empresa?
- ¿Tienen antivirus y firewalls en sus ordenadores los empleados que usan ordenadores portátiles u otros aparatos con acceso remoto?
- ¿Permite que sus empleados utilicen los ordenadores, sistemas o redes de la empresa con fines no laborales? Si lo permite, ¿deja usted claro que ciertos usos son inaceptables y pueden resultar en acciones disciplinarias?

- ¿Da cualquier tipo de formación o aprendizaje sobre seguridad a los empleados que usan los ordenadores o sistemas de información de la empresa?
- ¿Tiene algún tipo de política, norma o procedimiento relacionado con la seguridad?

Conocer sus obligaciones con el exterior (Responsabilidad)

- ¿Está familiarizado con los requisitos legales relacionados con cierto tipo de información (información de servicios financieros, información de salud, y todo tipo de datos que estén protegidos localmente por leyes o regulaciones incluyendo requisitos sobre datos personales, blanqueo de dinero o antiterrorismo)?
- Esto puede incluir tanto legislación sobre privacidad como regulaciones sectoriales.
- En algunos casos, especialmente cuando se posee información personal, delicada, o confidencial, se le requerirá cierto nivel mínimo de seguridad para proteger dicha información, sin tener en cuenta el tamaño de su empresa.
- ¿Está usted familiarizado con los derechos de los empleados en su lugar de trabajo?
  - Algunas leyes limitan su acceso a ciertos tipos de información y comunicaciones de sus empleados, o requiere notificación o consentimiento antes de que usted pueda acceder a la información, ya sea real o virtual, del empleado en su puesto de trabajo.
- ¿Es consciente de su rol en relación a la seguridad de terceros?
  - La seguridad de los sistemas de información es compleja porque las empresas están conectadas unas a otras directamente a través de Internet, creando interdependencias y ampliando el riesgo. No asegurar su sistema adecuadamente puede no solo comprometer y potencialmente dañar su empresa, puede también incrementar el riesgo de otros sistemas a los que usted esté conectado. Un riesgo importante resulta de la posibilidad de que un virus utilice su lista de contactos para propagarse o que usen su ordenador conectado a la red y sin protección para atacar o mandar spams a otros sistemas u ordenadores.

– Entienden sus empleados qué comportamiento es el adecuado en Internet? Esto va más allá de descargar o mandar material ilegal, inapropiado u ofensivo, e incluye toda conducta que no se adhiera a los valores y prácticas éticas de la empresa.

2_RESUMEN

Los cinco primeros pasos que hay que conocer sobre la buena seguridad de la información son:

1. Evaluar los objetivos de su negocio, las tareas que implican información y los activos cruciales para la información, por lo tanto, su riesgo.
2. Identificar y hacer un inventario de los activos cruciales para la información de su empresa.
3. Saber quién accede a dichos activos, cómo y por qué.
4. Encontrar un modo de mejorar la gestión de la seguridad de los activos de la información.
5. Enterarse de sus obligaciones frente a terceras personas en cuanto al uso de su información y frente a la sociedad como un todo.

Una vez dados estos pasos, estará usted en una buena posición para implementar algunos de los elementos de seguridad perfilados en la siguiente sección.

Lo que usted ha de hacer – elementos de seguridad

A continuación hay una serie de puntos que le ayudarán a diseñar, implementar, gestionar y continuamente reevaluar la estrategia de seguridad de la información de su empresa.

Política de seguridad (Diseño e implementación de la seguridad / Gestión de la seguridad)

Una política de la seguridad de la información clara y simple es esencial. Debe ser lo más corta posible –no más de una pocas páginas– y se debe entregar a todos los empleados. Dado que cada empresa es única, la política de seguridad de su empresa debe hacerse según las necesidades de su empresa.

La política debe incluir las siguientes afirmaciones:

- La información es vital para la empresa.
- Protegemos la confidencialidad, integridad y disponibilidad de la información crucial para nuestra empresa.
- Tenemos las siguientes normas que nos ayudan a conseguirlo:
  – seguridad física
  – seguridad personal
  – controles de acceso
  – tecnología de seguridad
  – respuesta y recuperación a los problemas de seguridad, y
  – auditorías de seguridad
- Tenemos procedimientos que nos ayudan a cumplir nuestras normas.
- Los empleados deben estar familiarizados con los procedimientos según su cargo y responsabilidades.
- Tomamos medidas disciplinarias contra los empleados que persistentemente o deliberadamente desobedezcan estas políticas, normas y procedimientos de seguridad de la información.

La política debería indicar dónde se pueden consultar los detalles sobre las normas y procedimientos.

Normas de seguridad (Diseño e implementación de la seguridad / Gestión de la seguridad / Respuesta / Nuevas evaluaciones)

Las normas mencionadas anteriormente en la sección de política de seguridad se examinan con más detalle a continuación.

Seguridad física (Diseño e implementación de la seguridad)

- Poner cierres apropiados u otro tipo de controles físicos en las puertas y ventanas de las salas donde se encuentran los ordenadores.
- Asegurar físicamente los ordenadores portátiles cuando no estén vigilados (por ejemplo, guardándolos por la noche en un cajón).
- Asegurarse y controlar todos los medios móviles relacionados con los activos cruciales para la información de la empresa, tales como: discos duros extraíbles, CD, disquetes y USB.

- Asegurarse de que se borra o quita toda información crucial de cualquier soporte o antes de deshacerse de él; CD o disquetes por ejemplo. Hay que tener en cuenta que borrar simplemente un archivo no es suficiente para hacer que éste sea irrecuperable.
- Asegurarse de que se borra o quita toda información crucial de cualquier ordenador antes de deshacerse de él.
- Guardar las copias de seguridad de la empresa físicamente fuera de la empresa o en un contenedor resistente al fuego y al agua.

Control de los accesos (Diseño e implementación de la seguridad / Gestión de la seguridad)

- Usar contraseñas únicas que no sean obvias (fechas de nacimiento o demás información fácil de imaginar y encontrar) y cambiarlas regularmente, preferiblemente cada tres meses.
- Usar contraseñas que contengan mayúsculas y minúsculas, números y caracteres especiales, y que tengan seis o más caracteres. Una ayuda es hacer que su contraseña sea una frase de la que se vaya a acordar en vez de una sola palabra.
- No anote su contraseña, y nunca la comparta con nadie. Si la tiene que compartir asegúrese de que se cambia lo más rápido posible, da igual cuánto confíe en la persona con la que ha tenido que compartir la contraseña.

Tecnología de la seguridad (Diseño e implementación de la seguridad)

- Todos los ordenadores que se utilicen en su empresa deben tener un antivirus instalado, y las definiciones de virus se han de actualizar como mínimo una vez a la semana (muchos antivirus tienen un icono de actualización rápida). Todo el tráfico entrante y saliente ha de ser escaneado por el antivirus, igual que cualquier disquete o CD que se utilice, incluso cuando proceda de una fuente «fiable». Como mínimo una vez al mes, y preferiblemente cada día, se debería hacer un escáner de virus en los ordenadores.
- Si sus ordenadores están conectados a Internet, y especialmente si usted usa una conexión de banda ancha, debe utilizar un software firewall. Esto le ayudará a prevenir la entrada de códigos perjudiciales a sus ordenadores que potencialmente puedan comprometer la con-

fidencialidad, integridad y disponibilidad de su red. También le ayudará a impedir que su sistema se use para atacar a otros sistemas sin su conocimiento. Los softwares firewall concebidos para que los usen personas no expertas están disponibles por precios razonables. Es posible que su sistema operativo, antivirus, o proveedor de Internet le ofrezcan un firewall. Hay revistas de consumidores que comparan las características y funciones de diferentes productos conocidos, por lo que representan una buena fuente de información. Existen firewall gratis, pero suelen requerir un conocimiento experto para su uso correcto.

- Actualizaciones / Parches del sistema: los softwares complejos siempre tienen vulnerabilidades. Los hackers pueden intentar explotar estas vulnerabilidades, y la única forma de protegerse es aplicando los «parches» que los vendedores del software proporcionan. Por ejemplo, los usuarios informáticos que aplicaron el «parche» de seguridad que se distribuyó para el «Sasser» fueron inmunes a ese ataque. Si es posible, configure su ordenador para que se actualice automáticamente de manera que se bajen los parches siempre que estén disponibles, o como mínimo asegúrese de que se aplican los parches tan pronto como sea posible.
- Si su empresa tiene una pequeña red interna conectada a Internet, debería considerar el uso de un hardware «todo en uno» que contenga un firewall, un antivirus y un sistema de detección de intrusos. Esto simplificará de gran modo el uso y mantenimiento de la tecnología básica para la seguridad en Internet.

Personal (Gestión de la seguridad / Conocimiento)

- Realizar controles de integridad a los nuevos empleados para asegurarse de que no le han mentido sobre sus antecedentes, experiencia o calificaciones.
- Dar a todos los nuevos empleados una simple introducción a la seguridad de la información, y asegurarse de que leen y entienden su política de seguridad de la información. Asegurarse de que saben dónde encontrar más detalles sobre las normas y procedimientos de seguridad de la información pertinentes para su rol y responsabilidades.
- Asegurarse de que los trabajadores únicamente tienen acceso a los activos que necesitan para desarrollar su trabajo. Si cambian de

puesto, asegurarse de que no siguen teniendo acceso a los activos que necesitaban para el puesto anterior. Cuando se despiden empleados, asegurarse de que no se llevan información crucial para el devenir de la empresa.

- Asegurarse de que ningún ex empleado tiene acceso a sus sistemas.
- Asegurarse de que los empleados conozcan los métodos típicos utilizados para comprometer los sistemas. Esto incluye e-mails que contengan virus y estratagemas de «carácter social» utilizadas por los hackers para explotar la amabilidad de los empleados para obtener información que le dará acceso a su sistema. Un ejemplo de estratagemas de «carácter social» es una llamada telefónica de un hacker haciéndose pasar por un ingeniero de mantenimiento del sistema o por un nuevo empleado.

Respuesta a incidentes en la seguridad (Respuesta / Nuevas evaluaciones)

- Un incidente en la seguridad es un acontecimiento que puede dañar o comprometer la confidencialidad, integridad o disponibilidad de la información crucial para la empresa o de los sistemas.
- Las vulnerabilidades de sus softwares son una fuente potencial de incidentes en la seguridad. Las vulnerabilidades deberían ser «parcheadas» tan pronto como sea posible una vez hayan sido anunciadas por el proveedor. Los proveedores de software lanzarán «parches» apropiados, descargables, a fin de acabar con las vulnerabilidades.
- Es importante hacer que su personal conozca los signos reveladores de los incidentes en la seguridad. Los signos serán los siguientes:
  - extrañas encuestas telefónicas, especialmente para obtener información
  - visitantes inusuales
  - comportamientos extraños de los ordenadores
  - apariencias inusuales de las pantallas de los ordenadores
  - mayor tardanza de los ordenadores para hacer las tareas rutinarias
- Su personal debe saber que siempre es aconsejable notificar a la persona indicada si se observa cualquiera de estos signos reveladores de la posibilidad de un incidente en la seguridad de la información.

- Si acontece un incidente, los empleados deberán saber con quién contactar y cómo.
- Deberá tener un plan para asegurar la continuidad de la empresa en caso de un serio incidente en la seguridad. El plan debería tener las siguientes especificaciones:
  - personas designadas para dar respuesta
  - contactos externos, incluyendo asesoramiento legal, bomberos y demás posibles expertos técnicos
  - planes de contingencia para incidentes previsibles tales como:
    - cortes de electricidad
    - desastres naturales y accidentes graves
    - robo de datos
    - pérdida de acceso al local
    - pérdida de empleados cruciales
    - fallo de los equipos
- Su plan debería llegar a todos los empleados y debería ser probado como mínimo una vez al año, incluso si no ha habido ningún incidente en la seguridad.
- Tras cada incidente que obligue el uso del plan, y tras cada test, el plan debería ser examinado y actualizado si fuera necesario utilizando lo aprendido en lo acontecido.
- La educación continua es vital.

Auditorías / Diligencia debida (Nuevas evaluaciones)

Una buena seguridad de la información incluye saber quién tiene acceso a sus sistemas y ser capaz de registrar dicho acceso. También hay que poseer un sistema que asegure que los procedimientos de seguridad se sigan en el día a día. La habilidad para auditar y evaluar la conformidad de la seguridad de la información es algo esencial, no se puede gestionar algo que no se puede medir.

- Debería auditar aspectos importantes de su seguridad, por ejemplo, quién tiene acceso a sus sistemas, y quién ha utilizado la información.
- Debería tener un registro de cada uno de los procedimientos de seguridad. Por ejemplo, si su procedimiento dice que se ha de hacer una

prueba de las copias de seguridad una vez a la semana, alguien debería registrar que se ha realizado dicha prueba. Guardar unos buenos registros es esencial para el control.

- Algunos controles pueden ser necesarios para propósitos legales o reguladores. Unos buenos registros pueden demostrar claramente que usted está cumpliendo con sus obligaciones.
- Una auditoría que evalúe si los procedimientos de seguridad de la información que la empresa tiene instaurados son efectivos y pertinentes. Es esencial volver a analizar y evaluar la efectividad de las normas y procesos de la seguridad de la información.
- Las auditorías solo son efectivas si se trabaja con los resultados y se identifican e implementan las medidas que se han de tomar.

Una buena auditoría no es solo un ejercicio escrito. Si algo no funciona, el resultado ha de decir qué es lo que no funciona y por qué. Esto ayudará a seguir mejorando la seguridad en su empresa.

3_EL CAMINO HACIA DELANTE

Si en su empresa se utiliza un ordenador, y si este ordenador está conectado a una red, la seguridad de la información ha de ser parte de su hacer empresarial. La seguridad de la información no es algo que solo tenga que ver con la tecnología, y no es algo solo para expertos. Se puede mejorar radicalmente la seguridad de su empresa –y de sus activos con los que hace negocio– tomando solo algunas pequeñas medidas. Usando contraseñas apropiadas, un firewall, antivirus y haciendo copias de seguridad regularmente mejorará significativamente la seguridad de su empresa y de aquellos que tratan con usted. Estos pasos requieren un esfuerzo inicial pero pronto se convertirán en algo natural para usted y sus empleados.

No hay un enfoque universal sobre la seguridad de la información, y no hay fórmulas mágicas. Los aspectos y recursos de la seguridad de la información para pequeñas empresas emprendedoras ayudan a los directivos a identificar y dar respuesta a los aspectos de seguridad que se puedan encontrar en su empresa. Todo el que use esta guía ha de adecuar a su empresa la política, las normas y los procedimientos de seguridad de la información. Cada empresa es única, y tiene su propio

conjunto de necesidades, recursos y circunstancias. Pero lo que toda empresa tiene, sin importar su tamaño o localización, es la necesidad de desempeñar un papel a la hora de crear una cultura global de seguridad.

La seguridad es un proceso continuo, no una cosa puntual. Instamos a que se dirijan a la página web de la ICC para más información relacionada con la seguridad procedente de expertos de todo el mundo, *Seguridad de la información, aspectos y recursos para la pequeña empresa emprendedora* es solo el punto de partida para lograr la seguridad en los negocios.

Para más información y recursos sobre seguridad de la información, por favor visite la página web de la ICC en www.iccwbo.org/home/menu_electronic_business.asp.

En qué consiste la seguridad

Rafael Ortega
Soci d'Ernst & Young

1_INTRODUCCIÓN

«Para quedarte donde estás debes correr lo más rápido que puedas, y si quieres ir a otro sitio debes correr por lo menos dos veces más rápido. (Lewis Carrol, Alicia a través del espejo*)»*

Esta frase, utilizada en libros de estrategia empresarial, escenifica literariamente el escenario en el que la seguridad de los sistemas y tecnologías de la información acometen su trabajo día a día en entornos empresariales, en los que procesos de negocio son informatizados y además se utiliza Internet como canal de comunicación con sus colaboradores o terceras partes.

El «time to market» hace que los sistemas que soportan los procesos de negocio estén más rápido en el mercado, nuevas tecnologías aparecen y se utilizan como factores diferenciadores o como elementos que incrementen la eficiencia de las compañías, adoptándolas inmediatamente en las compañías.

Pero ¿está todo probado de tal manera que se pueda asegurar la confianza necesaria para asegurar que el proceso sea confidencial, integro y esté disponible en cualquier momento y en cualquier lugar en el que se tenga que desarrollar?

Creo que antes de empezar a desarrollar el apartado, es necesario no olvidar una serie de principios de seguridad que si bien tienen años, no por ello, han perdido vigencia.

- **La seguridad no es un valor absoluto.** ¿Alguien puede decir que mi valor de seguridad es 5 y esto significa que es imposible que tenga algún incidente de seguridad? Si me pregunta mi Dirección General como estamos de seguros ¿puedo responder 10 sobre10?

- **No se puede hablar de un sistema informático que sea seguro sino más bien que no se conocen tipos de ataque que puedan vulnerarlo.** No hay que hacer muchos comentarios sobre este tema, la disciplina informática se ha «vulgarizado», su conocimiento ya no está en un reducido grupo de personas, que accedían a documentación restringida y era muy difícil tener un conocimiento muy profundo de los sistemas llamados «propietarios».Hoy está todo en la red, desde manuales a sistemas, utilidades y programas, que, sin muchos conocimientos informáticos pueden utilizarse como elementos de análisis y ataque. Cualquier tecnología que se use masivamente es exhaustivamente estudiada para identificar fallos de programación que ocasionen agujeros de seguridad.
- **El último eslabón de la seguridad descansa en la confianza en alguna persona.** Por mucho que se realice una correcta segregación de funciones, que se utilicen tecnologías de seguridad que impidan el acceso a los datos por parte de las personas que administran las infraestructuras tecnológicas y, que por tanto, pueden realizar cualquier operación sobre los sistemas, siempre alguien puede realizar acciones malintencionadas. El ejemplo más claro de este principio es la paradoja del becario, en el que en una empresa, que hasta el Consejero Delegado tiene unas medidas de seguridad acordes a las necesidades de la organización, existe en el área de informática un becario de una empresa subcontratada, con permiso de administrador, que podría tener accesos privilegiados.
- **El personal usuario de los sistemas de información constituye el eslabón más débil en la cadena de la seguridad,** puesto que sus actuaciones, no alineadas con las buenas prácticas en seguridad, pueden acarrear importantes impactos en la misma.

Pero lo principal es darse cuenta que la seguridad es una actitud, yo en cuanto me siento en el coche me pongo el cinturón de seguridad…inconscientemente, como un hábito. Fíjense en estos ejemplos que pongo a continuación:

- *¿Cierra la puerta con llave cuando sale a comprar algo*? ¿Por qué no bloquea su PC cuando se levanta a hacer algo?
- *¿Conecta usted la alarma cuando sale a cenar?* Entonces, ¿por qué no establece una contraseña para proteger el acceso a sus documentos confidenciales?

- *¿Cierra el gas para evitar fugas y preservar su casa?* Entonces, ¿por qué no saca copias backup de sus ficheros personales, almacenados en su ordenador personal?

El reto de la seguridad es la implantación de un entorno de control que impacte mínimamente en los procesos de negocio y que estos se conviertan en tareas habituales del trabajo. Es decir, el objetivo es proporcionar confianza, sin reducir la eficiencia.

¿Es un problema actual la seguridad de Internet? La respuesta debe ser contundente, NO. Es necesario revisar las hemerotecas y no olvidar la historia, porque como dice el dicho, aquel que la olvida está condenado a repetirla. ARPANET, nacida en 1969, estaba pensada para la disponibilidad, es decir, asegurar que la Red continuase funcionando aunque algún nodo estuviese indisponible. Todos los protocolos que gestionaban la red fueron diseñados sin pensar en la seguridad, su objetivo era la sencillez de la comunicación, es decir la funcionabilidad.

Ya, en 1986 se identificó el primer agujero de seguridad por parte de Cliff Stoll del Lawrence Berckeley National Laboratory. Dos años después, se produjo el primer ataque organizado, denominado el gusano de Morris y afectó al 10% de los ordenadores conectados a la red. Este hecho disparó las alarmas de seguridad y fue el detonante para la creación del CERT (Computer Emergency Response Team) que fue creado por la Universidad Carnegie Mellon, expandiéndose por las universidades europeas a principios de los 90, siendo en 1995 cuando se crearon los dos primeros CERTs españoles.

En 1989 un código malicioso (el gusano Sank/Oilz) colapsó los ordenadores conectados a la Red con Sistema Operativo VMS (sistema propietario de los ordenadores Digital) aprovechando un agujero de seguridad. A partir de 1994, aparecieron utilidades informáticas que permiten capturar y analizar la información que circula por la red.

El robo de tarjetas de crédito se incrementa a partir de 1999, ya sea por la explotación de fallos en los sistemas o por fallos humanos en la administración de los elementos tecnológicos que trataban los datos de dichas tarjetas.

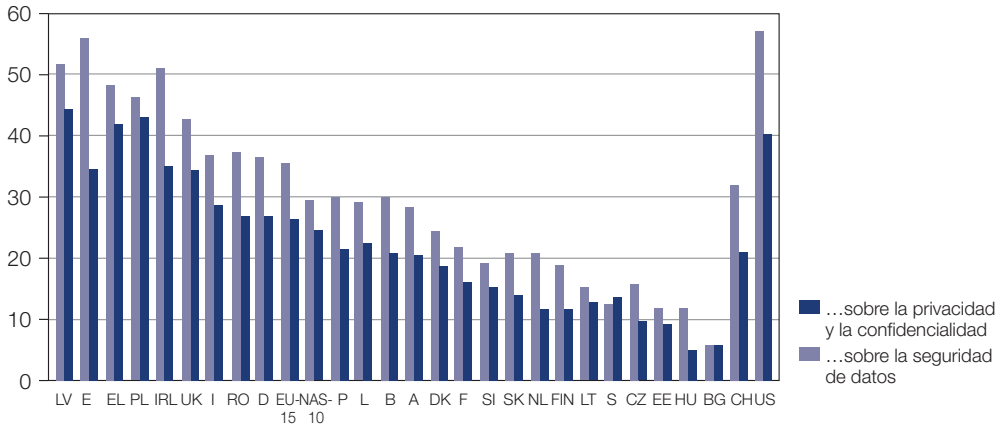
Se puede ver que a partir de ese año, surgen iniciativas con el objetivo de proporcionar confianza a las transacciones electrónicas, que finaliza con la publicación en el 2005 de las directrices que VISA y MASTERDCARD

publican con la denominación PCI DSS (Payment Card Industry Data Security Standard) que en un posterior apartado se explicará.

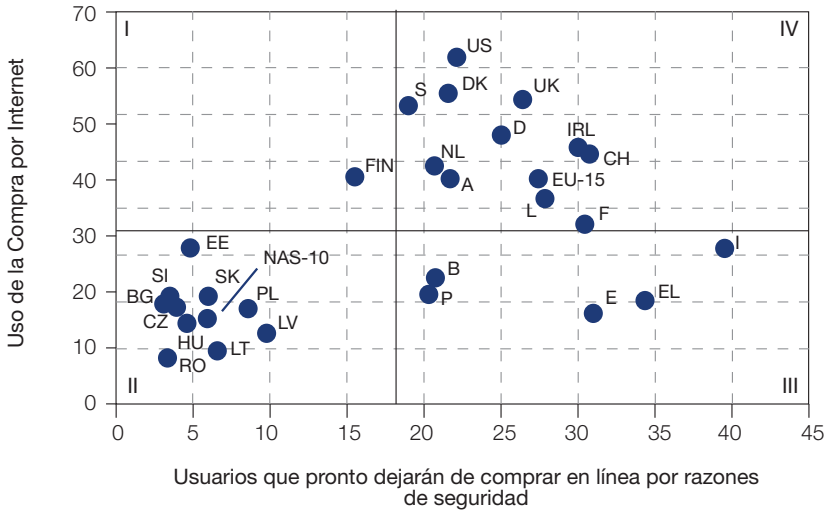
Todos estos datos y la alta preocupación por los temas concernientes a la seguridad hacen, que precisamente este aspecto del comercio electrónico, estudio tras estudio, no sea uno, sino el inhibidor más importante para que la velocidad de introducción en las empresas y la sociedad en general, no haya sido la más deseada.

Como ejemplo, indicamos los indicadores obtenidos en un estudio encargado por la Unión Europea, dentro del programa SIBIS (Statistical Indicators, Benchmarking the Information Society), publicándose el informe final en el 2003 (http://www.sibis-eu.org/statistics/stat_ind.htm).

Preocupación social en materia de seguridad.
(Pesos indicados en porcentajes)



Efecto de la seguridad sobre el comercio electrónico (%)



2_AMENAZAS Y SU EVOLUCIÓN

España registró el pasado mes de enero el 6 % de todos los ataques de «phishing» padecidos por el conjunto de las entidades financieras del mundo, según un informe de la empresa RSA, la división de seguridad de la compañía de protección de datos EMC.

De esta manera, España, que en diciembre registró el 2% de los ataques, vuelve a ocupar el tercer lugar en la clasificación de países afectados por el «phishing» a entidades financieras. El número de bancos españoles víctimas de esta agresión informática fue siete, con un total de 62 ataques, todos ellos provenientes de Estados Unidos y Belize.

En cuanto a los datos mundiales, el número total de ataques se ha reducido el mes pasado el 21,4%, ya que hubo 161, frente a 205 en diciembre, aunque «el número de bancos atacados ha vuelto a los niveles de noviembre».

http://www.vnunet.es/Actualidad/Noticias/Seguridad/Privacidad/20070228020

Por Agencias [28-02-2007]

En 1983, tres años antes del primer problema grave en la red, se estreno la película «Juegos de Guerra» (Wargames), con un Mathew Broderick, casi bebé, en el que su personaje es un adolescente que con un gran conocimiento en informática y electrónica, abusa de estos para introducirse en sistemas ajenos para conseguir nuevos videojuegos, hasta que en su búsqueda se conecta a un ordenador del ejercito que tiene la misión de controlar las armas nucleares estadounidenses para evitar el fallo humano. La película gira en el momento en el que el juego se convierte en un caso real y activa todos los sistemas nucleares. En esta película, el acceso a los sistemas se basa, entre otros, en la rotura de claves, debido a la falta de políticas de contraseñas, ¿les suena?

Datapro Information Services Group era una división del grupo de empresas McGraw-Hill, compradas posteriormente por Gasnert Group, que suministraba información y análisis detallados y actuales sobre el espectro global de productos de IT, proveedores, tecnologías y mercados. Datapro Information Services Group realizaba encuestas anuales entre los profesionales de seguridad de la información, con bases de datos obtenidas del Computer Security Institute, la revista BYTE, y las de las em-

presas suscritas a Datapro. El cuestionario lo componían preguntas sobre el tamaño y complejidad de sus instalaciones, su política de seguridad, cuales son sus principales preocupaciones con respecto a seguridad en IT, qué incidentes han sufrido, y qué medidas tenían implantadas.

En el informe de 1995, la preocupación principal entre los encuestados durante 1995 fueron los virus y los códigos maliciosos (caballos de Troya, gusanos, etc.). Otras preocupaciones importantes eran el acceso no autorizado a sistemas/redes, accesos a Internet, exposición de contraseñas, y el robo de equipos informáticos.

En cualquier encuesta de seguridad actual, estos dos temas son prioritarios todavía, aunque se vea, hoy en día, a situaciones más especificas. Así la primera preocupación se concreta dentro de los temas de fraude electrónico, además de los problemas que ocasionan en la disponibilidad de la información y los segundos dentro del entorno de la gestión de identidades de accesos.

Si hay una conclusión que se puede extraer de estos 24 años transcurridos, es que el objetivo del ataque no ha cambiado pero sí las técnicas, que han evolucionado, llegando a un nivel de sofisticación extrema.

Lo que si ha cambiado, y por fin en España hemos sido conscientes de ello, es que los «malos» existen y están organizados. Hay grupos organizados que realizan sus delitos desde la sustracción monetaria, espionaje empresarial/industrial, subastas de vulnerabilidades de los sistemas en la red, etc. Ya no eran esos «románticos» cerebros que, al final del día, aportaban su conocimiento a la comunidad.

Estas organizaciones delictivas, trabajan con el objetivo fundamental del robo de las identidades de los usuarios, intentado con métodos de engaño y abuso de confianza (ingeniería social) o con métodos técnicos aprovechando vulnerabilidades de los sistemas conocer o sustraer los datos de autenticación y firma, datos de tarjetas de crédito de estos sobre los sistemas de banca electrónica y otros entornos transaccionales en el que es posible un quebranto económico. La práctica totalidad de problemas de fraude electrónico en la banca electrónica se basa en la sustracción de identidades.

Existen diversas formas de agrupamiento de las distintas amenazas sobre estos elementos, pero como ejemplo de un modelo sencillo y comprensible, es interesante la descrita por el Catedrático de Ciencias

de la Computación e Inteligencia Artificial de la Universidad Carlos III, D. Arturo Ribagorda en su libro Seguridad y Protección de la Información. En él agrupa estas amenazas en cuatro grandes tipos: Intercepción, Modificación, Interrupción y Generación.

INTERCEPCIÓN. La más difícil de detectar y la más fácil de producir. Se origina cuando una persona, programa, proceso, etc. logra acceso a una parte del sistema a la que no está autorizado (escaneo de red, copias no autorizadas de programas, etc.).

MODIFICACIÓN. Además del acceso se cambia en parte o en su totalidad el funcionamiento del sistema accedido y sin autorización (cambio de líneas de programa, base de datos).

INTERRUPCIÓN. Fácil de detectar y difícil de luchar. Esta puede ser temporal o permanente. La interrupción puede contemplar la destrucción física o lógica de los elementos.

GENERACIÓN. Posibilidad de incluir campos y registros en base de datos, virus (programas completos en un sistema), líneas de programa, etc.

Una clasificación exhaustiva de las amenazas que sufren los usuarios de la Red y de los sistemas de información, estaría desfasada al día siguiente, pero creo interesante al menos describir las más importantes desde el punto de vista que afecta a los usuarios de los ordenadores personales:

- *Adware:* software utilizado para la distribución de contenidos publicitarios, su introducción en el sistema no ha sido autorizada por el usuario y muchas de estas aplicaciones espían el seguimiento del usuario por la red.
- *Bot:* diminutivo de Robot. Es un programa diseñado para automatizar tareas. Utilizado de forma maliciosa permite que un intruso controle un ordenador remoto. Los BOTs se pueden utilizar para mandar spam, descargar y guardar archivos ilegales, atacar a otros ordenadores, robo de información, etc. A los ordenadores infectados por BOTs se les suele llamar «ordenadores zombis».
- *Botnet:* red de BOTs. Grupo de ordenadores infectados por BOTs y controlados de forma centralizada.
- *Hoax (enganys):* intento de hacer creer a un grupo de personas que algo falso es real. Su objetivo es saturar las redes de comunicaciones, hacer creer a los usuarios que están infectados por algún tipo de virus, saturar el correo electrónico, etc.

- *Malware:* término utilizado para describir de forma genérica cualquier tipo de software o código malicioso.
- *Phishing:* ataque de ingeniería social que tiene como propósito la obtención de información personal sensible del usuario, como contraseñas a la banca electrónica y los códigos de firma, números de tarjetas de crédito. La forma de realizar el ataque es el uso del envío masivo de correos electrónicos en el que el atacante se hace pasar por una persona o empresa de confianza (sobre todo entidad financiera) pidiendo de forma aparentemente legítima dicha información sensible. El ataque también se puede realizar por medios de mensajería instantánea o incluso por medios telefónicos.
- *Rootkit:* herramientas diseñadas para controlar de forma oculta, sin que el usuario pueda detectarlo, un ordenador. La utilización de rootkits no debería ser necesariamente maliciosa, ya que son herramientas útiles para la administración remota de los sistemas.
- *Spyware (programas espía):* aplicaciones que recopilan información sobre una persona u organización sin su conocimiento. Esta información se envía a un punto de recolección y control. El *spyware* se distribuye como parte de otro programa (como un caballo de Troya), como a través de un gusano, o de páginas Web que explotan vulnerabilidades de los navegadores.
- *Caballo de Troya:* programa que aparentemente realiza una función, pero que en realidad realiza otra. No siempre es malicioso o destructivo, pero sus propósitos suelen ser:

  – Borrado de ficheros y discos duros.

  – *Keylogger* (registro de las pulsaciones que se realizan sobre el teclado)

  – Acceso remoto al ordenador (puertas traseras, etc.)

- *Virus:* Programa que se replica a sí mismo de forma exacta o con modificaciones (mutaciones), en otra pieza de código ejecutable. Los virus pueden utilizar diversos tipos de anfitriones:

  – Ficheros ejecutables.

  – Sectores de arranque.

  – Ficheros de *scripts*.

  – Macros de documentos.

- Cuando un virus se inserta en un código ejecutable, le garantiza que se «explotará» cada vez que se ejecute dicho código ejecutable y a su vez se propagará buscando ficheros limpios en el anfitrión para infectarlos. Los virus se pueden distribuir a través de ficheros, a través de redes vía ficheros compartidos, en documentos y en los sectores de arranque de los discos. Para que sea clasificado como virus, el código simplemente se tiene que replicar.
- *Gusanos:* los gusanos es un subconjunto de los virus. Tienen la habilidad de replicarse por si mismos sin ayuda de personas. Típicamente, los gusanos explotan vulnerabilidades en los servicios de red de los sistemas, por lo que se propagan rápidamente entre sistemas vulnerables. Probablemente, el tipo de gusano más común es el que utiliza el correo electrónico para transportarse. Es este caso, el correo electrónico no está infectado, pero transporta el gusano.

En la siguiente figura vemos otro tipo de amenazas de seguridad que son comunes y hacen que la seguridad de la información sea vital para aportar confianza a los procesos de negocio.

Falsificación de información para terceros	Bombas lógicas
Agujeros de seguridad de redes conectadas	Ingeniería social
Indisponibilidad de información clave	Empleados descontentos
Interceptación de comunicaciones	Virus, troyanos...
Software ilegal	Mails “anónimos” con información crítica o con agresiones
Acceso indebido a documentos impresos	Robo de información
Robo o extravío de pdas, portátiles	Spam o Correo basura
Intrusión en Sistemas Informáticos	Destrucción de equipamiento
Destrucción de soportes documentales	Violación de contraseñas
Interrupción de los servicios	Incumplimiento de leyes y regulaciones
Propiedad de la Información	Intercepción y modificación de e-mails
Fraudes informáticos	Violación de la privacidad de los empleados

3_MODELOS DE SEGURIDAD

«Es muy sencillo tener un sistema seguro. Simplemente tiene que desconectar todas las conexiones remotas y permitir únicamente los

terminales directamente conectados, colocar la máquina y sus terminales en una sala protegida, y un guardia en la puerta.»

F.T. Grampp & R.H. Morris.

Esta era la realidad no hace mucho años, todo bajo la llave de un único grupo de personas que custodiaban los datos de las compañías. Hoy en día para procesar y almacenar datos con unas necesidades de seguridad extremas se sigue utilizando el método descrito arriba. Ejemplos de este tipo de medida de seguridad son las entidades raíz de una jerarquía de certificación. Aunque después de ver a Tom Cruise vulnerar un sistema como el que describimos, en Misión Imposible I, ya no se sabe como asegurar completamente los sistemas.

Bromas a parte, los modelos de seguridad han evolucionado desde el clásico en el que las tres características básicas de seguridad (confidencialidad, integridad, disponibilidad) se desdoblaban para definir más atributos que describan mejor las necesidades de seguridad de los procesos de negocio y las transacciones electrónicas.

Una de las primeras cuestiones que hay que resolver es determinar el nivel de protección de la información, para ello plantéense las siguientes cuestiones:

¿Qué medidas se están tomando para proteger la información? Identificar que activos no se encuentran protegidos.

¿Qué debe hacerse para proteger la información? Situación de la empresa con respecto al conjunto de medidas definidas como necesarias, comparando la situación actual con la idónea.

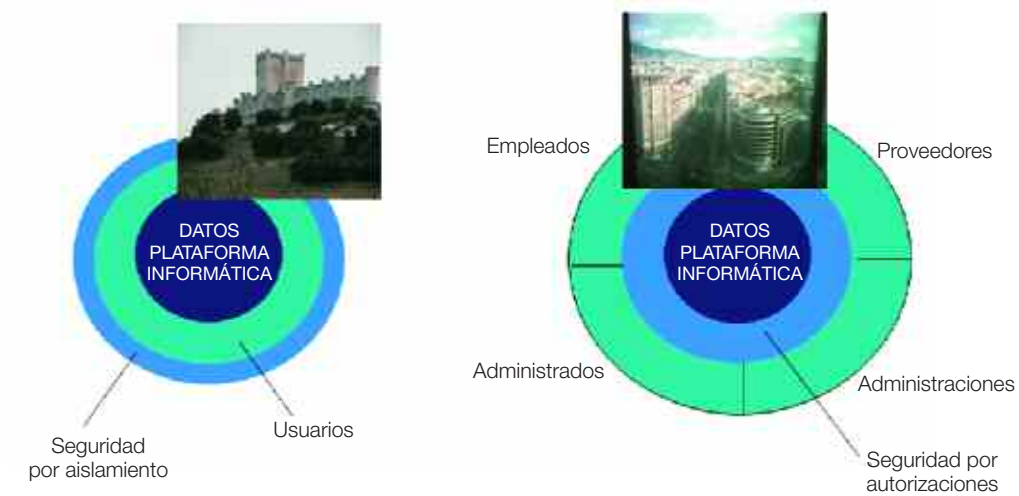
¿Qué puede hacerse para proteger la información? Medios, tanto económicos como humanos, disponibles para la implementación de un nivel de seguridad aceptable. Los recursos asignados dependerán de la importancia que se otorgue a la seguridad de la información.

¿Quien debe hacer qué para proteger la información? Asignación del personal que estará involucrado en el programa de seguridad previamente acordado. Las tareas de seguridad serán responsabilidad tanto de las personas encargadas de la seguridad de los programas como de los usuarios finales, que deberán tener sus propios requerimientos y responsabilidades de seguridad.

Si todas las preguntas tienen respuesta, uno tiene un Plan de Seguridad.

3.1_Modelo de McCumber

Así mismo y debido a la evolución de los sistemas de información, la estrategia de seguridad de las empresas, ha cambiado radicalmente. Estábamos en un entorno en el que solo los usuarios accedían a un sistema central donde estaban todos los sistemas de información, y accedían a través de redes «privadas» y con un aislamiento del perímetro era más que suficiente, es decir se tenia un estrategia de defensa tipo castillo. En la actualidad hemos abierto las puertas a todos nuestros colaboradores (proveedores, accionistas, clientes), hemos derribado las murallas y estamos en el medio del campo (recordad el dicho de quien puede poner puertas al campo…), ¿podemos pensar en una ciudad, poner una muralla y dejar todo el interior abierto? Coches, viviendas, tiendas. Impensable, esto hace cambiar el concepto y pasar a una defensa por autorizaciones, en donde las organizaciones deben controlar qquién accede, cuándo accede, cómo accede, qué información puede conocer, qué funciones puede realizar, qué registros deben generarse. Gráficamente se puede representar:



Es importante conocer que existen modelos de seguridad que nos permiten implantar la seguridad de una forma sistematizada, así, el primer modelo de seguridad con el que trabajé fue uno que descubrí en una revista americana y que me pareció sencillo, comprensible, práctico y fácil de usar. En la actualidad no ha perdido vigencia y se ha implantado en algunas organizaciones, ampliando los atributos de seguridad. Este

modelo lo presentó John R. McCumber lo expuso en la decimocuarta edición de la National Computer Security Conference, es independiente del entorno, arquitectura o tecnología que gestiona nuestra información. Su aplicación puede ser universal y no está restringido por diferencias organizacionales.

Naturaleza de la información

Hablar de la naturaleza de la información es referirse a un concepto excesivamente abstracto. Algunos lo definen como el libre flujo de conocimientos, otros como la inteligencia que debe ser custodiada.

La información puede estar en tres estados: Proceso, almacenamiento y transmisión.

Concretando más, se puede decir que el procesamiento es una combinación del almacenamiento y la transmisión, pero para este modelo, es fundamental tener esta distinción entre los tres estados y aplicar el modelo de forma adecuada. Por ejemplo, el cifrado de la información sirve para proteger la confidencialidad y la integridad en la transmisión de la información o para el almacenamiento en soporte magnético, sin embargo, es necesario que la información esté en claro para su procesamiento. Por tanto el procesamiento es un estado fundamental de la información que requiere medidas de seguridad específicas.

Características de la Información

- Confidencialidad de la información

La confidencialidad de la información es el corazón de la política de seguridad del sistema de información.

La confidencialidad de la información pretende que una persona acceda solo a la información que debe conocer y hacer con ella solo lo que le este permitido. Es decir, disponer de una política de seguridad que defina sujetos y objetos y determine a que objetos pueden acceder dichos sujetos. La confidencialidad es tener la seguridad que se ha realizado una completa implantación del control de accesos de acuerdo con la clasificación de la información realizada en la organización.

- Integridad de la información

Es quizás la característica de la información más compleja e incomprendida. Si se define como activos que pueden ser modificados por partes autorizadas, esta definición estaría confinada a un mero control de accesos.

Una definición más exacta puede ser la que expone McCumber: la define como el grado de confiabilidad del contenido de la información, definida en calidad y no como quien tiene o no tiene acceso a ella. Integridad es calidad de información identificada como fiel reflejo del dato que representa en realidad.

La definición de integridad debe comprender los términos de exacta, autorizada y completa.

- Disponibilidad de la Información

Esta característica provee a los usuarios autorizados la información cuando es requerida o necesitada. Es decir la información debe de ser siempre recuperable en caso de pérdida o imposibilidad de uso de los sistemas de información de la organización.

Cuando las medidas de seguridad fallan, las medidas de disponibilidad de la información son las que entran en acción. Las medidas de disponibilidad de la información intentarán minimizar el impacto que se produce cuando existe una imposibilidad de uso de la información.

En este momento el modelo dispone de una matriz en la que el eje de abscisas corresponde a los estados de la información y el eje de ordenadas a las características de la información. Pero todavía el modelo es incompleto.

Medidas de seguridad

Es necesario definir el tipo de medidas a implantar para asegurar las distintas características de la información a través de sus distintos estados.

Con la matriz que se ha creado, actualmente hay definidas 9 intersecciones, es decir 9 campos de actuación para definir medidas de seguridad en función de sus características y su estado. Por ejemplo, medidas que garanticen la confidencialidad de la información en el estado de transmisión.

Podemos ver que tecnológicamente, la solución a esta intersección, en la matriz, seria el cifrado de la información, por lo que uno comenzaría por definir que tipo de algoritmo de cifrado utilizará y una vez decidido el tipo de cifrado, analizar los productos que existen en el mercado. Esto se puede repetir con las otras ocho celdas, pero aún el modelo está incompleto, porque falta acompañar a las medidas tecnológicas, las normas y procedimientos de uso y la concienciación y formación.

- Medidas tecnológicas

El nivel tecnológico es el primer nivel de la tercera dimensión definida. Este tipo de medidas es la base para las otras dos. Para este modelo se pueden definir las medidas tecnológicas como dispositivos físicos o lógicos que son usados específicamente para asegurar las características de la información a través de los distintos estados.

Las organizaciones se han construido alrededor de las responsabilidades, pero parece que las necesidades tecnológicas de las organizaciones se han establecido para acomodar las nuevas maquinas en función del proceso, almacenamiento y transmisión, en vez de las necesidades de la propia información. Es decir, la organización se ha adaptado para seguir la evolución tecnológica. Esto hace parecer que la tecnología existe para la tecnología. Hay que tener en cuenta que los ordenadores y las telecomunicaciones, son simplemente soportes para la información.

Es necesario adaptar esos medios a las características de la información. Con esto pasamos al siguiente nivel.

- Normas y procedimientos

No es posible esperar que los avances tecnológicos vayan solucionando todos los problemas que surgen en los sistemas de la información. La adopción de normas y procedimientos de seguridad puede solucionar inmediatamente estas carencias en la seguridad de la información, que la tecnología no soluciona.

Es necesario acompañar a la tecnología implantada de un conjunto de normas de actuación, procedimientos de trabajo y uso. La experiencia en la realización de diagnósticos de seguridad, dice que la mayoría de los puntos débiles encontrados son debidos a la falta de normas y procedimientos.

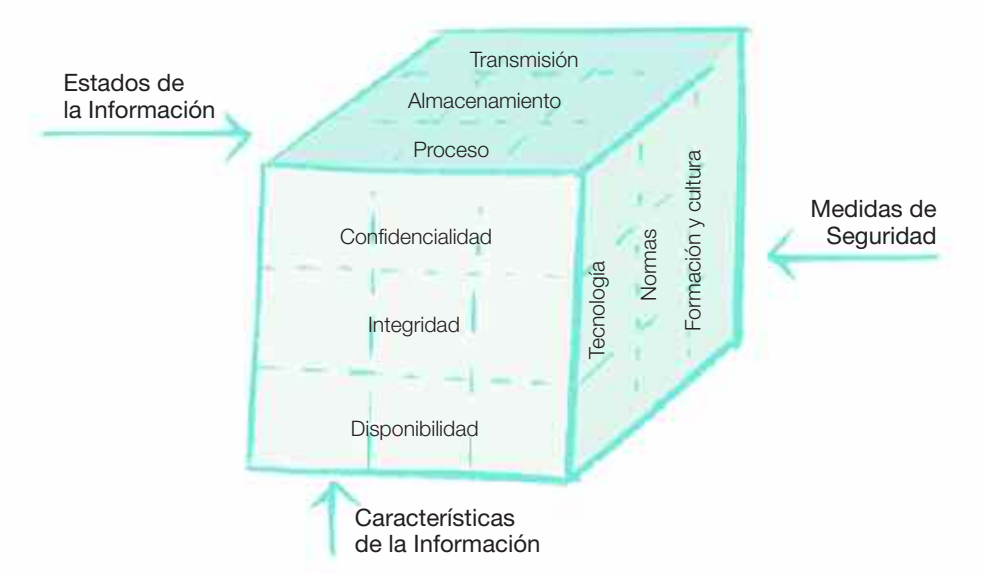
Estos dos niveles de la mencionada tercera dimensión representan el diseño y la aplicación de los sistemas de seguridad de la información. El último nivel de esta dimensión es la comprensión necesaria para proteger la información.

- Concienciación y formación

Este tipo de medida puede convertirse en la más importante medida de seguridad y desde luego, absolutamente imprescindible. Comenzando por la comprensión de la seguridad, por parte de todos los componentes de la organización, para seguir por el análisis de las amenazas y vulnerabilidades, y la implantación posterior de todas las normas y procedimientos de seguridad, hace que la seguridad de la información se convierta en cultura de la organización, objetivo final que se debe perseguir cuando se decide implantar un Plan de Seguridad de la Información.

El modelo de Seguridad

El modelo de tres dimensiones se convierte en un cubo con 27 celdillas como marco de actuación.



A partir de este modelo se puede definir la seguridad de la información como todas aquellas medidas tecnológicas, de normas y procedimientos y de concienciación que aseguran la confidencialidad, integridad y

disponibilidad de la información en sus estados de proceso, almacenamiento y transmisión.

No siempre será necesario actuar en cada una de ellas, pero conviene analizarlas previamente a la elaboración de cualquier Plan de Seguridad de la Información para conseguir un resultado realmente eficaz y no pasar por alto ningún aspecto que afecte a la seguridad.

Como es evidente, vale poco la acumulación de medidas encaminadas a la protección de un determinado aspecto, si otros quedan totalmente olvidados. En más de una ocasión se observan medidas aplicadas sin esa visión global, y el resultado final presenta debilidades incomprensibles para cualquier profesional de la seguridad.

No es un problema que dependa de la cuantía de la inversión, sino del equilibrio en su aplicación. Cuando ocurre un incidente, cualquiera no llega a comprender como se ha podido producir el incidente sobre uno de sus activos más vitales (información), cuando la inversión a realizar supone proporcionalmente tan poco. La cuestión está en determinar donde y como deben aplicarse las medidas de protección.

Este modelo, no solo debe servir para construir un modelo de seguridad a implantar en la empresa, sino también como una herramienta de evaluación de la situación actual de la seguridad.

Cada vulnerabilidad descubierta puede llevar implícita un medida de seguridad a implantar correspondiente en su celdilla del cubo o si se asume el riesgo de la materialización de dicha vulnerabilidad.

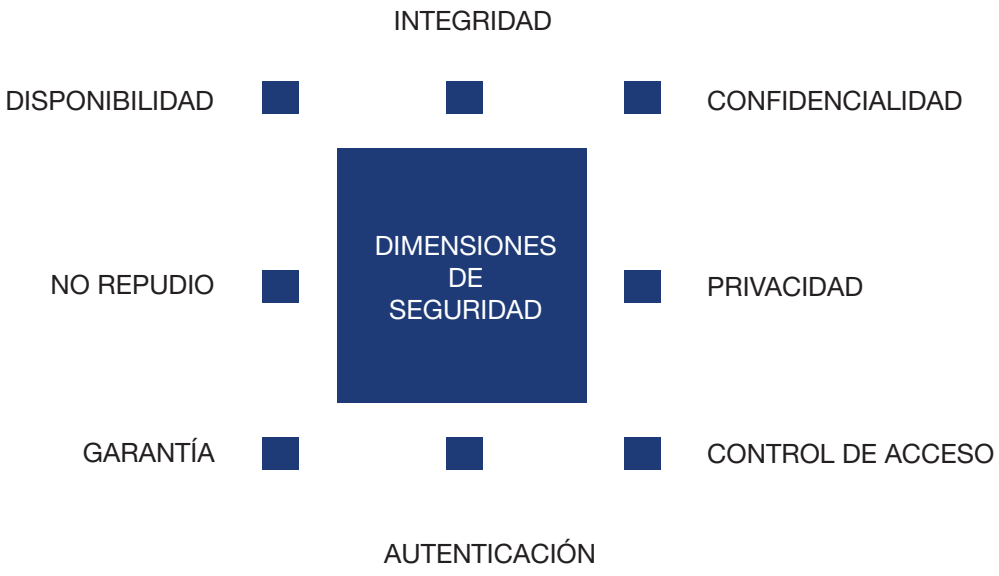
Unos años después, algunos autores, empezaron a plantearse la necesidad de ampliar el modelo más allá de estás tres características de la información, ya que la problemática evolucionaba, la transmisión de datos, el uso de base de datos y la asignación de propietarios de esas base de datos, con una legislación en cada país, hace necesaria más características de la información que acoten mejor la arquitectura de medidas de seguridad a implantar. M. Parker, en la conferencia que impartió en la 14th National Computer Security Conference con el titulo»Restating the Foundation of Information Security» propone el desdoblamiento de las características tradicionales en:

- Confidencialidad-Posesión.
- Integridad-Autenticidad.

- Disponibilidad-Utilidad.
- Las nuevas características se definen de la siguiente manera:
- Posesión: Tenencia o propiedad y control.
- Autenticidad: Conforme a los hechos y a la realidad, válido, verdadero o cierto, real y genuino para un propósito.
- Utilidad: Útil para un propósito.

Un ejemplo, de este desdoblamiento es el caso del robo y destrucción de un portátil que contenga ficheros cifrados. En él no se ha perdido la confidencialidad, ya que el delincuente no podrá ver su contenido. En caso de tener copia backup (cosa no muy habitual), la disponibilidad e integridad tampoco resultarían afectadas, el propietario va a perder la posesión exclusiva de la información contenida en su portátil.

Estos fueron los primeros pasos en los que el concepto en que la seguridad se puede acotar a la confidencialidad, integridad y disponibilidad se quedaban escasos para las nuevas necesidades de seguridad de la información, estos se están desdoblando en otros *atributos o dimensiones* de seguridad que nos permite acotar las necesidades de seguridad de las transacciones electrónicas que automatizan los procesos de nuestro negocio. Un esquema de estos puede ser el siguiente:



Definiéndose como:

- **Integridad:** no variación indeseada de los datos
- **Confidencialidad:** los datos solo los conoce quien está autorizado
- **Privacidad:** la tenencia de datos esta justificada
- **Control de Accesos:** por necesidades y responsabilidades
- **Autenticación:** quien accede es quien dice ser
- **Garantía:** el sistema hace lo que se espera
- **No repudio:** el autor de un hecho no puede negar la autoría del mismo
- **Disponibilidad:** está accesible cuando se necesita

Todo esto es ocasionado por un cambio de paradigma en la seguridad:

En estos años transcurridos, uno de los aspectos fundamentales en los que ha evolucionado el sector de la seguridad de la información es la estandarización. Existen diversos organismos en los que el esfuerzo en divulgar estándares técnicos, metodologías, buenas prácticas ha sido considerable y enriquecedor para el mercado. Sobresalen por su importancia la ISO/IEC (International Organization for Standarization/ International Electrotechnical Comisión) y el NIST (National Institute of Standards and Technology) de Estados Unidos.

3.2_ISO 17799

El ISO/IEC, viene realizando un trabajo de emisión de buenas prácticas y estándares de seguridad, a través del JC1 Subcomité 27. Desde mi punto de vista, el más importante y base para cualquier estructuración exhaustiva de la seguridad en una organización, proceso, sistema de información o infraestructura tecnológica es el ISO/IEC 17799:2005, código de buenas prácticas de seguridad.

El estándar proviene del BS 7799 publicado en su primera versión por The British Standard Institute (BSI) en 1995. Revisado en 1999 y dividido en 2 partes:

BS 7799-1: Parte I: «Código de Práctica para la Gestión de Seguridad de la Información».

BS 7799-2: Parte II: «Especificaciones para el Sistema de Gestión de Seguridad de la Información».

Durante el año 2000, la Parte I «Código de Práctica para la Gestión de Seguridad de la Información» fue adoptada por la Organización Internacional para Estandarización (ISO), debido a que el Reino Unido presentó su estándar para su aprobación por un trámite rápido, obteniendo los apoyos necesarios para conseguirlo. De tal manera que la BSI 17799: Parte I, pasó a ser ISO/IEC 17799.

A raíz de esta decisión, BSI modificó su segunda parte, y lo publicó en Septiembre de 2002, con el objetivo de tener una norma de certificación.

En España, se traduce la norma y se adopta como UNE-ISO/IEC 17799 y se publica en el 2002 y ya en el 2004, basado en el BS 7799-2:2002, se pública la norma UNE 71502, con la obligación del desarrollo dentro del sistema de gestión de un sistema de indicadores.

En este momento en España existía la posibilidad de certificarse contra dos marcos de referencia el BSI y la UNE, pero con una diferencia fundamental, mientras las certificaciones del sello BS, estaban acreditados por la autoridad nacional británica de acreditación, UKAS (United Kingdom Accreditation Service), las entidades españolas que certificaban bajo el prisma de la norma UNE, su sello no estaba acreditado por el ENAC (Entidad Nacional de Acreditación) creándose una confusión el mercado sobre los valores y diferencias entre la acreditación y su valor en el mercado.

Ya sea por razones políticas o por razones técnicas, debido al descontento de algunas personas y en contra de lo habitual, en la que una norma no se puede revisar hasta pasados los cinco años de su revisión, se consiguió iniciar en Abril de 2002, un proceso de «revisión temprana» durante la reunión internacional del SC27 de Berlín. Este proceso duró 3 años en el que se revisaron, discutieron y aprobaron unos 4.500 comentarios, para finalizar con la publicación de la ISO/IEC 17799:2005 (futura ISO 27002). Este estándar emite especificaciones de un SGSI. Establece las especificaciones para **establecer, operar, mantener y mejorar** el Sistema de Gestión de Seguridad de la Información (SGSI). Es decir, el marco de referencia para la certificación.

El nuevo estándar es un documento muy claro y estructurado, siendo una guía clara y detallada para construir un entorno de control de seguridad, siendo independiente pudiéndose acometer su aplicación desde

un punto de vista global en la compañía, un proceso o departamento, en un sistema de información o en la infraestructura tecnológica. Las «Clauses» o dominios de control se describen por un objetivo general, los 11 dominios se representan en la siguiente figura:

ISO/IEC 17799:2005 - Código de buenas prácticas

Establece 39 objetivos de control y 134 controles agrupados en 11 categorías o dominios.

Cada Dominio, se divide en un subconjunto de controles (133) que para una mejor comprensión se han desarrollado tres apartados descriptivos:

- **Control:** descripción del control especifico, que de su correcta implantación se consigue cumplir con el objetivo de control del dominio.
- **Guía de implantación:** Desarrollo en detalle de cómo implantar el control para poder cumplir con el objetivo del Dominio
- **Otra Información:** información adicional de ayuda, como por ejemplo, referencia a otros estándares.

Los controles que se consideran claves en este estándar son:

Controles de carácter legislativo y regulatorio

Derechos de propiedad intelectual (apartado 15.1.2). Claramente identifica la obligación de proteger los derechos de propiedad intelectual

y derechos de software propietario, es decir, no pueden existir «copias piratas» de ningún tipo en las organizaciones y es necesario controlar que los usuarios de la infraestructura tecnológica no utilicen software no legalizado por la compañía.

Salvaguarda de registros organizativos (apartado 15.1.2). Uno de los controles más importantes y a la vez más abiertos. Hay que proteger cualquier registro organizativo (independiente del formato que tenga) contra perdida, destrucción o falsificación, en función de las necesidades del negocio, legales, etc. Hay que asegurar la disponibilidad de los registros «vitales» de la compañía y su integridad contra la falsificación, por lo que se ven implicados varios controles más y políticas generales de la empresa, como por ejemplo la de copias de salvaguarda (backups de soportes), plan de continuidad e, incluso, la firma electrónica.

Protección de datos y privacidad de información de carácter personal (apartado 15.1.2). Ningún comentario al respecto porque se tratará más en profundidad en apartados posteriores.

Controles basados en buenas prácticas:

Política de Seguridad (Apartado 5 completo). Control clave que debe ser aprobado por la alta dirección. Es decir, la política afectará a todos las personas que jerárquicamente estén por debajo de la persona que lo firme, nunca se podrá aplicar a áreas paralelas o superiores. Es por esto que se pide que sea refrendada por los órganos más altos de la empresa.

Un punto fundamental y muchas veces de equivoco por su traducción a nuestra lengua es el término «policy», que aparece en el estándar. En los países anglosajones, este término contiene, lo que en nuestro país y en muchos entornos latinos, la política general de la compañía que no viene a ser más que un compromiso formal de la Dirección con respecto a la Seguridad de la Información y la normativa general de seguridad, que recoge los códigos, conductas y preceptos de seguridad que deben ser implantados en la organización, en los sistemas e infraestructuras tecnológicas, de obligado cumplimiento para todos los participantes en el entorno empresarial. Si bien la primera debe ser fija, la segunda es la que puede ser modificada y debe ser revisable periódicamente (apar-tado 5.1.2)

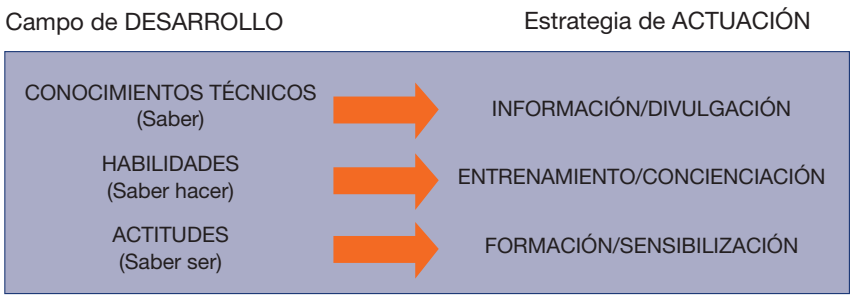
Asignación de las responsabilidades de la Seguridad de la Información (Apartado 6 completo). Fundamentalmente y desde mi punto de vista, la clave para el cumplimiento de este dominio, no es tener un departamento de seguridad, o un director de seguridad de la información, es identificar todas las tareas de seguridad que se necesitan realizar en la compañía para cumplir los objetivos de seguridad (entorno de control de seguridad), organizarla con un enfoque a procesos, asignar responsabilidades de las mismas y fijar registros e indicadores de cumplimiento.

No siempre la organizaciones no tienen los recursos suficientes (económicos o humanos) y/o el suficiente conocimiento para la implantación y mantenimiento de un control, en un modelo de gestión de riesgos, la Dirección deberá asumir el riesgo o decidir traspasarlo (por ejemplo, pólizas de seguros), de tal forma que la vulnerabilidad debida a la falta del control deberá ser monitorizada con el objetivo de dar una respuesta rápida y de esa manera intentar reducir el impacto en caso de materialización de la amenaza.

Es un punto clave la formalización de la relación con terceras partes, proveedores, clientes, grupos de interés, etc. Todo lo que no este reglado bajo compromisos aprobados o firmados no vale. Se debe dirigir y controlar la seguridad en sus relaciones con el entorno, identificando y evaluando los riesgos y realizando una correcta gestión del mismo. Por ultimo, cabe destacar la obligación de realización de evaluaciones independientes del nivel de control de la seguridad implantado, es decir, obligación de auditorias independientes. EL QUE DEFINE, DISEÑA E IMPLANTA NO AUDITA.

Concienciación y formación de seguridad (apartado 8.2.2). Aspecto clave de la seguridad en el que todas las compañías están haciendo un especial esfuerzo. Antes de que la ISO 17799 fuese un referente en el mercado, el Reglamento de Medidas de Seguridad, que desarrollaba la Ley de Protección de Datos, ya obligaba a la difusión de las medidas de seguridad implantadas en el entorno de los datos de carácter personal.

En la siguiente figura representamos los tres niveles que se pueden realizar para el cumplimiento de este control, desde la sensibilización, concienciación y divulgación:



DIVULGACIÓN: *(no presencial)*	*Plan de comunicación específico sobre los aspectos técnicos de la seguridad, utilizando canales de información (intranet, etc.) con amplio alcance y con posibilidad de testar si los usuarios han leído la información y si han asimilado los contenidos (evaluable e interactivo).*
CONCIENCIACIÓN: *(presencial)*	*Sesiones de corta duración (cuatro horas) de corte técnico/tecnológico en las que se pretende que el público objetivo entienda el qué, el por qué y los comos de funcionamiento de los sistemas de seguridad para inducir a los usuarios a un comportamiento alineado a las necesidades de los sistemas.*
SENSIBILIZACIÓN: *(presencial)*	*Sesiones de una jornada en la que la monitorización pretende mover las actitudes de los asistentes para que exista en la organización un compromiso activo con la seguridad informática y los usuarios lo incorporen a modo de hábito, en su "día a día" profesional.*

Reporte de incidentes de seguridad (apartado 13.1). Objetivo perteneciente al dominio (clause) definido como Gestión de incidentes, que se divide en dos objetivos de control: Notificación y Gestión y Mejora. Este objetivo es fundamental en toda estrategia de seguridad y sobre todo en una organización que esté abierto a Internet, ya que, en un entorno de mejora permanente, es la única forma de poder tener un proceso eficaz de prevención, detección y actuación ante incidentes y debilidades de seguridad.

Este objetivo establece que debe desarrollarse, implantarse y, sobre todo, divulgar, todos los aspectos relacionados con los incidentes y debilidades que las *personas identifican*, es decir, todo aquel que está involucrado en algún proceso de negocio o tecnológico de la empresa, incluidos las terceras partes participantes en ellos, deberán participar en la consecución de este objetivo.

El objetivo se divide en dos controles: Reporte de los eventos de seguridad de la información y reportes de debilidades de seguridad.

En este dominio, el siguiente objetivo, Gestión y Mejora (13.2), se divide en tres controles: Procedimientos y responsabilidades, aprendiendo de los incidentes de seguridad y recopilación de evidencias. Este objetivo de control, exige el desarrollo e implantación de procesos de gestión de incidentes, la asignación de responsabilidades, la creación de entorno tecnológicos que permitan el estudio y análisis de impacto de los incidentes de seguridad, es decir, gestionar el riesgo. Así mismo, el último control

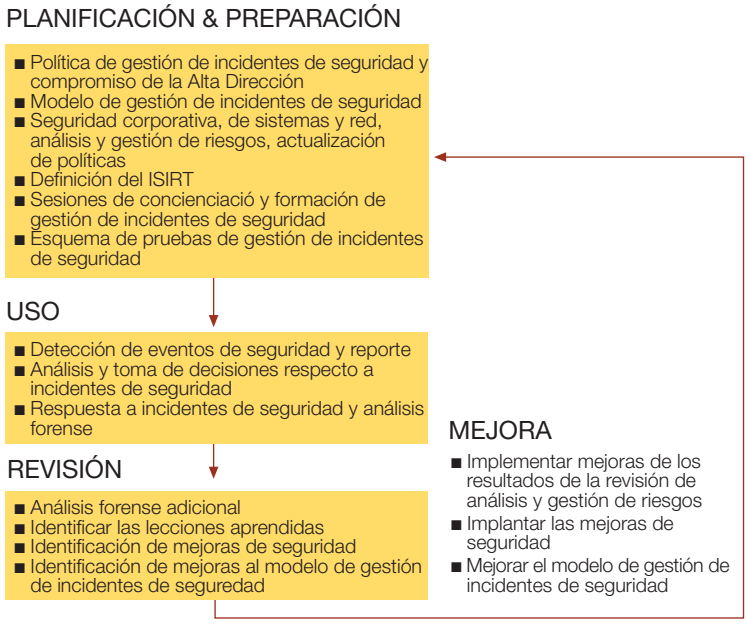
se refiere a un aspecto fundamental de dicha gestión, el análisis forense y la cadena de custodia de las pruebas para poder realizar acciones judiciales.

Este dominio se completa con el estándar ISO/IEC 18044:2004 Information Security Incident Management, que establece como desarrollar un proceso completo de Gestión de Incidentes de Seguridad. El estándar se desarrolla en torno a estas dos definiciones:

- »Un *evento o incidencia de seguridad* es un estado identificado en un sistema, servicio o red que indica una posible violación de la política de seguridad, un fallo de los controles de seguridad, o una situación previamente desconocida que pueda tener relevancia para la seguridad»
- »Un *incidente de seguridad* es uno o varios eventos inesperados de seguridad que tienen una alta probabilidad de comprometer la operativa del negocio y que amenaza la seguridad de la información»

En la siguiente figura resumimos el contenido del estándar:

ISO/IEC 18044:2004



Gestión de la continuidad del negocio (apartado 14). Las exigencias que el mercado y el «anywhere, anytime», por el que los participantes en el ecosistema de las organizaciones, utilizan los recursos físicos y lógicos que los procesos clave de la compañía utilizan con soporte para su desarrollo, hace que el cumplimiento de esté control sea clave en cualquier estrategia de seguridad.

¿De seguridad?, existe un tendencia, debida a la masiva utilización de ITIL (the IT Infrastructure Library), un método de organización de los servicios de IT, basado en el concepto de Servicios y procesos, en el que la disponibilidad y continuidad del servicio no son procesos ligados a la seguridad, sino a la prestación del servicio.

En muchas organizaciones, sobre todo en el sector financiero, la continuidad de negocio no de pende de seguridad, ni tan siquiera de IT y las personas que lo desarrollan, apenas tienen conocimientos de IT y están más ligados a áreas de negocio (organización, operaciones, medios).

Volviendo al estándar, dicho dominio se divide en cinco controles:

- **Incluyendo la seguridad de la información dentro del procesos de gestión de la continuidad de negocio.** Con este control se describen someramente, los pasos necesarios para obtener los recursos (económicos, organizacionales, técnicos, ambientales, etc.) que aseguren la continuidad de los procesos clave de la organización. Entre ellos, se exige el cálculo del impacto que la imposibilidad de realización de dichos procesos tiene en la organización, la identificación de los activos que son utilizados por estos, su priorización en función de su criticidad, la identificación e implantación de controles preventivos que permita mitigar dicho impacto. Es decir, realizar lo que comúnmente se conoce un BIA (Business Impact Analisys). Así mismo, se define la necesidad de desarrollar la documentación necesaria para dar respuesta antes un desastre, realización de pruebas, procedimientos para mantener el plan al día y la necesidad de considerarlo como un proceso más del negocio, con responsabilidades claramente definidas y con un nivel de aprobación y gestión adecuado a la importancia que tiene dicho proceso.
- **Continuidad de negocio y evaluación de riesgos.** Todo el proceso de definición de necesidades para desarrollar un eficaz proceso de continuidad del negocio, debe realizarse desde un punto de vista de gestión del riesgo, que nos permita identificar posibles escenarios de desastre y de esta manera definir los medios de respuesta en caso de materializarse alguna de las amenazas, identificadas.
- **Desarrollando e implantando planes de continuidad incluyendo la seguridad de la información.** En este control, a la vez que habla de aspectos ligados a la seguridad, como el aseguramiento de la dis-

ponibilidad de la información, la necesidad de proteger los activos de la información contra vulnerabilidades y la propia disponibilidad de la documentación de gestión del plan; enumera los requisitos para la implantación del plan (documentación, evaluaciones, pruebas).

- **Planificando un marco de trabajo de la continuidad de negocio.** Todo lo descrito en los anteriores controles deben estar organizados bajo un marco de trabajo (metodología) que incluya condiciones para activar el plan, procedimientos de emergencia, planes alternativos de trabajo en caso de desastre, procedimientos temporales de recuperación y restauración, procedimientos de vuelta a la normalidad, planificación del mantenimiento de este, concienciación y divulgación; identificación clara de responsabilidades individuales y disponibilidad de los recursos para poder ser utilizados en caso de desastre.
- **Probando,** manteniendo y reevaluando los planes de continuidad de negocio.

Por la importancia que tiene este control, clave para la supervivencia de las organizaciones, **British Standards** ha publicado un estándar para el desarrollo de Planes de Continuidad de Negocio, el BS25999: 1-2006. Este estándar define los procesos, principios y una terminología común para el desarrollo y gestión de un plan de continuidad sea cual sea el tamaño de la organización, además de proporcionar un conjunto de controles exhaustivo basado en las mejores prácticas de la BCM, así como su ciclo de vida

El BS25999: 2-2006 (sin publicar en la actualidad) especifica los requisitos para definir, implantar, operar, monitorizar, revisar, mantener y mejorar un sistema de Business Continuity Management en el contexto de riesgos globales de negocio en una organización y la implantación de los controles de continuidad de negocio adaptados a las necesidades particulares de cualquier empresa.

El estándar define «La gestión de la Continuidad de Negocio» (BCM) como un proceso de gestión que identifica los impactos potenciales que amenazan a una Organización y que proporciona y marco de actuación para la fortaleza (*resilence*) del edificio y la capacidad para una respuesta efectiva que salvaguarde los intereses de sus principales *stakeholders*, reputación, imagen de marca y sus actividades de creación de valor»

En la siguiente figura se enumeran los apartados del estándar:

1. Alcance y aplicabilidad
2. Términos y definiciones
3. Visión de la Gestión de la Continuidad de Negocio (BCM)
4. Política de Gestión de la Continuidad de Negocio
5. Gestión del programa BCM
6. Conocer la organización
7. Determinar las estrategias de continuidad
8. Definir e implantar una respuesta BCM
9. Probar, mantener y revisar los acuerdos BCM
10. Asimilación del BCM en la cultura de la organización

Los apartados clave en el desarrollo de un plan son :

- **Alcance y aplicabilidad (apartado 1).** Se debe definir el propósito del plan, es decir, proporcionar una base de conocimiento, desarrollo e implementación de un plan de continuidad de negocio. El estándar no cubre las actividades de los planes de emergencia ni las emergencias civiles.
- **Política de Gestión de la Continuidad de Negocio (apartado 2).** Se definen *2* procesos: establecimiento de actividades para definir la capacidad de continuidad de negocio y operación diaria y mantenimiento de dicha capacidad. Así mismo, el contenido de la política debe contener: el ámbito y alcance del BCM (definición clara de limitaciones y exclusiones), recursos asignados al BCM, definición de principios, guías y estándares para el BCM; referencias a estándares relevantes, regulaciones o políticas; revisión continua y regular y actividades externalizadas: evidencia (auditada) de acuerdos BCM efectivos.
- **Gestión del programa BCM (apartado 5).** Como alcanzar los objetivos definidos en la Política de BC a través de un flujo de trabajo definido en 3 fases: asignación de responsabilidades, implantación de la continuidad de negocio en la organización gestión continúa del BCM.

La documentación a gestionar y mantener es:

- Política BCM
  - – Declaración del alcance BCM
  - – Términos y referencias
- Análisis de impacto de negocio (BIA)
- Análisis de Riesgos y Amenazas
- Estrategia/s BCM
- Programa de concienciación
- Programa de capacitación o formación
- Planes de gestión de incidentes
- Planes de Continuidad de Negocio
- Planes de Recuperación de Negocio
- Calendario e informes de las pruebas
- Acuerdos de Nivel de Servicio (SLA) y contratos

El flujo de trabajo se representa en la siguiente figura:

- **Conocer la organización (apartado 6).** El objetivo del apartado es Identificar los productos y servicios clave y las actividades y procesos críticos que los soportan. Para ello se deberá realizar un Análisis de

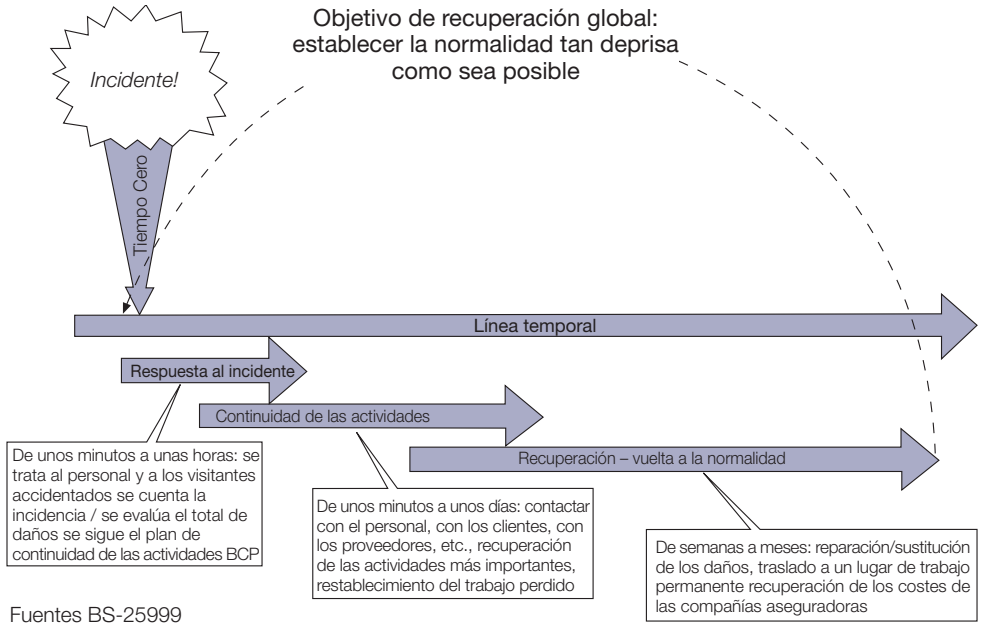
Impacto (BIA), evaluando y documentando el impacto de la interrupción de las actividades que soportan los servicios y productos clave la compañía. Así mismo, para cada actividad (definida en el alcance), se deberá definir el periodo máximo de interrupción tolerable. Hay que identificar las actividades interrelacionadas, activos, infraestructura y recursos que también necesarios Evaluación de amenazas sobre actividades críticas (análisis de riesgos) y la selección de alternativas (gestión del riesgo)

- **Determinar las estrategias de continuidad (apartado 7).** El objetivo es evaluar estrategias de recuperación para personas, instalaciones, tecnología, información, suministros y stakeholders. La estrategia dependerá de el máximo periodo tolerable de interrupción de la actividad crítica, los costes de implantación y las consecuencias de no hacer nada.
- **Definir e implantar una respuesta BCM (apartado 7).** El objetivo es desarrollar el proceso de respuesta a incidentes, contemplando la definición de un equipo de respuesta y desarrollando los planes, procesos y procedimientos; además de desarrollar los procedimientos de activación, operación, coordinación y comunicación de la respuesta a incidentes. Se tiene que definir planes específicos para recuperar o continuar las operaciones estado «normal» (Planes de recuperación), con los siguientes contenidos:
  - Contenido general de los Planes (gestión de incidentes, continuidad y recuperación)
  - Objetivo y alcance
  - Funciones y responsabilidades
  - Procedimiento de invocación
  - Propietario y «mantenedor» del plan
  - Datos de contacto
- **Definir e implantar una respuesta BCM (apartado 8).** El apartado indica los procedimientos a desarrollar en el proceso de respuesta a incidentes en el que se tiene que definir los equipos de respuesta, la existencia de planes, procesos y procedimientos y los procedimientos de desactivación, operación, coordinación y comunicación de la respuesta a incidentes y la definición de los planes específicos para recuperar o continuar las operaciones estado «normal» (Planes de recuperación). El contenido general de los planes (gestión de incidentes, continuidad y recuperación) será:

– Objetivo y alcance
– Funciones y responsabilidades
– Procedimiento de invocación
– Propietario y «mantenedor» del plan
– Datos de contacto

Así mismo, el plan de gestión de incidentes deberá contener información adicional con respecto a un plan de acción y lista de tareas, contactos de emergencia, actividades del personal (evacuación, servicios de emergencia, asistencia sanitaria, etc.), respuesta a medios de comunicación gestión de stakeholders, ubicación para la gestión del incidente y anexos (registros vitales, etc.).

Con respecto a la información adicional al del Plan de Continuidad de Negocio (BCP), la información adicional debe estar compuesta por los planes de acción y lista de tareas, requerimientos de los recursos, personal responsable (continuidad y recuperación) y anexos con información complementaria (listado de proveedores, etc.).



Fuentes BS-25999

• **Probar, mantener y revisar los acuerdos BCM (apartado 9).** El objetivo del apartado mantener las capacidades del BCM, para ello se deben definir las pruebas del Plan con objetivos claramente definidos y documentando el resultado de las pruebas, indicando las recomendaciones necesarias para la mejora del plan y la planificación de las mismas.

Se deben, mantener los acuerdos BCM, definiendo y documentando un programa y el desarrollo de un programa de mantenimiento con evidencias documentadas de una gestión preactiva, que verifique que el personal clave está entrenado, capacitado y con evidencias documentadas que los cambios en la Organización han sido incorporados a los planes de continuidad y de gestión de incidencias.

- Por último, se deben revisar los acuerdos BCM, documentando los intervalos de revisión (plan de revisión formal), cumpliendo con la política del BCM acorde a la regulación aplicable, estándares y buenas prácticas, realizando auditorias o recabando la opinión independiente cualificada (internas o externas), autoevaluaciones.

- **Asimilación del BCM en la cultura de la organización (apartado 10).** El objetivo de esta apartado es conseguir que BCM se convierta en parte de los valores principales y modelo de gestión de la Organización, ya que la principal amenaza es la falta de concienciación del personal acerca del BCM. Todo esto se debe realizar mediante programas de Concienciación con la definición de un programa que contenga además del plan de actuación la evaluación de su eficacia, la capacitación de las habilidades necesarias y la formación práctica, incluyendo la participación activa en las pruebas

Además de estos controles obligatorios, en los entornos en el que los sistemas se abren a otros participantes externos, el dominio 11 de Control de Accesos, es imprescindible para asegurar los recursos que se «abren al exterior».

El control de accesos es un proceso como tal, que se divide en tres subprocesos: Autenticación, autorización y administración de autorizaciones. Dicho de otra forma, el proceso que una persona realiza para acceder a los recursos u objetos que necesita para desempeñar sus funciones dentro de una organización, comienza por la identificación/autenticación en un mecanismo destinado para tal fin. La persona física se identifica en dicho mecanismo y corrobora que es él el que quiere acceder a los recursos/objetos, mediante **la autenticación**.

Una vez que el usuario se ha autenticado, es decir «es realmente quien dice ser», hay que autorizar al usuario el acceso a «algo o a realizar algo». ¿Como se autoriza a la persona este acceso a los recursos/objetos?, mediante un mecanismo de *autorización*. Este mecanismo se compone

de un monitor de referencia que consulta una base de datos de autorizaciones, para determinar si el usuario que intenta realizar una operación está autorizado a realizarla. Las autorizaciones de la base de datos deben ser administradas y mantenidas por «alguien», es decir, debe estar correctamente implantada la política de autorizaciones de la organización *(administración de autorizaciones)*.

Habida cuenta, como se ha indicado anteriormente que, en la actualidad, la gran mayoría de los ataques a sistemas o usuarios, tienen el objetivo del robo de credenciales, para suplantar a los usuarios legítimos, la autenticación es un proceso vital para asegurar la confiabilidad de los sistemas.

Un buen informe acerca de las tecnologías que aseguran el servicio de autenticación es el «Federal Information Processing Standards Publications (FIBS PUBS) 190: Guideline for the use of Advanced Authentication Technology» del National Institute of Standards and Technology (NIST). Este documento «proporciona información y guía a las Agencias Federales en el uso de tecnologías avanzadas de autenticación como un elemento crítico en el diseño de mecanismos de control de acceso efectivo para sistemas automatizados que procesan información no clasificada».

Aunque la definición de autenticación abarca la verificación de la identidad, autenticación del mensaje origen y autenticación del contenido del mensaje, creo que en este apartado vamos a limitarnos en la autenticación de usuarios, aplicados a personas humanas.

Dicha guía define tres métodos para verificar la identidad de un usuario basado en:

- Algo que el usuario conoce y no conoce nadie más, es decir, nuestra querida palabra de paso.
- Algo que el usuario posee, por ejemplo, una tarjeta con banda magnética, en la que están grabados sus datos de identificación/autenticación.
- Alguna característica física, como la huella dactilar, la voz.

En el pasado, y debido a que la mayoría de los puntos de entrada a los sistemas estaban en lugares físicos determinados y con un sistema de control de acceso a estos recintos, con el uso del sistema de autenticación mediante palabra de paso era suficiente. Por supuesto, las amenazas internas se creían controladas con este tipo de sistema.

En la actualidad, hay un común acuerdo: el sistema de autenticación utilizando palabras de paso no es todo lo fiable que las necesidades de seguridad actuales demanda.

El concepto de autenticación fuerte, se define como el uso, en el proceso de acceso a las aplicaciones, de dos de los sistemas definidos anteriormente.

En el caso de autenticación mediante algo que se posee, la denominación común es la de «Token». Token es un objeto físico único para un usuario o un grupo de usuarios que almacena la información necesaria para realizar el proceso de autenticación mediante un protocolo determinado.

Los tokens pueden trasmitir la información de autenticación, mediante interfaces de contacto o sin contacto. Las primeras son las más comunes y se basan en dispositivos de lectura o lectura/escritura conectados a la estación de trabajo (lectores de tarjetas magnéticas, tarjetas inteligentes). Las interfaces sin contacto se basan en la transmisión de la información de autenticación, a través de infrarrojos o radiofrecuencia, a dispositivos conectados a la estación de trabajo.

Existe otro tipo de transmisión de la información, utilizando al usuario como «interfaz de comunicación de la información de autenticación». Estos tokens poseen una pantalla que comunica al usuario la información de autenticación y éste la introduce en la estación de trabajo, a través del teclado.

Por la capacidad de proceso, podemos diferenciar los siguientes tipos de tokens:

- **Tarjeta de banda magnética.** En la banda magnética está almacenada la información de autenticación.
- **Tarjetas inteligentes o criptográficas (smart cards).** Contienen un chip en el que se guarda la información de autenticación, y se accede a esta mediante la introducción de un PIN para autenticar que la persona que quiere acceder a la tarjeta es la que realmente es.
- **Tokens con microprocesador**. Estos tipos de dispositivos son las conocidas «calculadoras». Se accede a la información de autenticación, ya sea directamente (solamente es un dispositivo de almacenamiento) o el microprocesador contiene un programa que genera la información necesaria para realizar el proceso de autenticación.

- **Tokens software.** La información de autenticación es almacenada o generada mediante un programa al cual se accede por medio de la introducción de un PIN.

Este tipo de soporte para la autenticación tiene como complemento el uso de contraseña dinámica (one time password), es decir la contraseña o palabra de paso no puede ser usada más que una vez. Es decir, en el servidor de autenticación existe un algoritmo que genera claves distintas cada cierto periodo de tiempo, estos generadores están sincronizados con el token de usuario. Así mismo, las tarjetas criptográfica, son el soporte para certificados digitales (X.509) para autenticase en las aplicaciones mediante diversos protocolos de autenticación (Kerberos, Sesame, etc.) o firmar transacciones para evitar el repudio de la misma.

Con respecto a los sistemas de autenticación biométricos no vamos a extendernos mucho, ya que en la actualidad su uso se restringe a sistemas clasificados, ya que su coste es actualmente sigue siendo alto para ser implantado en compañías con gran número de usuarios.

Para elegir un sistema de este tipo hay que tener en cuenta dos tipos de valores: el FAR, Ratio de Falsa Aceptación o de tipo 2 (representa el porcentaje de usuarios no autorizados que son correctamente identificados como usuarios validos) y el FRR, Ratio de Falso Rechazo o de tipo 1 (usuarios autorizados que han sido rechazados).

A nivel de los procesos ligados a la autorización, existen desde hace bastantes años, modelos reconocidos y que se implantan fácilmente en las organizaciones y aplicaciones

Partiendo del siguiente concepto: «un sistema se considera seguro si impide la transferencia de derechos de acceso a usuarios no autorizados», comenzaremos viendo los tipos de control de acceso clásicos.

Control de accesos discrecional

El propietario de un recurso tiene el privilegio de proporcionar acceso a otros usuarios a este recurso.

Este modelo se ocupa únicamente de controlar el acceso del usuario al recurso, sin preocuparse de lo que el usuario realiza con el recurso.

Control de accesos obligatorio

En el caso de este tipo de control de accesos, cada usuario y recurso tiene asignado un nivel de seguridad. Cada nivel de seguridad asociado con un recurso u objeto refleja la sensibilidad de los datos o información que contiene el recurso.

El nivel de seguridad asociado con un usuario, también llamado autorización, refleja el compromiso de los usuarios a no revelar información sensible a usuarios no autorizados de verla.

Este sistema jerárquico es el más comúnmente utilizado tanto en el entorno militar como en el entorno civil, asignando diferentes niveles de seguridad (secreto, confidencial, clasificado, etc.).

El acceso a un recurso u objetos por un usuario es garantizado si y solo si existe alguna relación entre los niveles de seguridad de los dos.

Los modelos de seguridad obligatoria se dividen en modelos multinivel y modelos de flujo.

Modelos Multinivel

En los modelos multinivel realizamos agrupaciones de los usuarios y los recursos en grupos con características comunes. Por ejemplo, los usuarios se agrupan por departamentos y los recursos por objetos que son utilizados por un proceso de negocio. Estas agrupaciones de usuarios y recursos se denominan compartimentos.

A cada recurso individual se le asigna un nivel de confidencialidad. Por lo que cada recurso está identificado por un par de coordenadas: pareja de nivel de confidencialidad y compartimento. Luego, como se puede comprobar, estamos realizando una clasificación de los recursos.

Igualmente, los usuarios también se les puede definir un nivel de confidencialidad o nivel de autoridad, con lo que, también los tenemos identificados por un par de coordenadas, y por tanto clasificados.

Entre los usuarios y los recursos se debe establecer algún tipo de relación. Un ejemplo puede ser que un usuario puede acceder a un recurso si y solo si el nivel de autoridad del usuario es mayor o igual al nivel de ese recurso. La relación algebraica particular entre usuarios y recursos se denominan retículos.

Modelos de Flujo de la Información

En este modelo se describen los «caminos» autorizados para el flujo de información de un sistema. En este «camino» debe especificarse que usuarios pueden acceder a los recursos dependiendo del nivel de clasificación, siendo este nivel de clasificación el mismo que hemos definido en el modelo multinivel (nivel de autoridad para usuarios y nivel de confidencialidad para recursos) que se les haya definido.

La variante que aporta este modelo es que define modos de acceso: sólo lectura, lectura/escritura, solo escritura.

Dentro de este tipo de modelo podemos distinguir otros dos tipos en función de las relaciones de acceso que se establecen.

Modelo de Bell La Padula

La relación que establece este modelo, es que un usuario solo puede leer recursos u objetos con un nivel de confidencialidad inferior o igual a su nivel de autoridad, y solo puede escribir en los recursos u objetos con nivel de confidencialidad mayor o igual a su nivel de autoridad . Evidentemente, un usuario puede leer y escribir en recursos u objetos que tengan su mismo nivel de autoridad.

En otras palabras: se prohíbe la lectura hacia arriba y la escritura hacia abajo. En este modelo se establece que los recursos y usuarios no pueden cambiar sus niveles de confidencialidad y autoridad, ya que están preestablecidos de antemano (»principio de la tranquilidad»).

Modelo de Biba

Este modelo completa la deficiencia del modelo de Bell-La Padula con respecto a la integridad de la información.

En el modelo de Biba se establecen además niveles de integridad o de utilidad para los recursos y usuarios, aunque para los usuarios se define como nivel de autoridad.

Las dos relaciones que se establecen son las siguientes:

Un usuario puede escribir en un recurso si este posee un nivel de autoridad mayor o igual al nivel de integridad o autoridad del objeto.

Si un usuario puede leer un recurso u objeto con un determinado nivel de integridad, también puede escribir en el resto de recursos u objetos con niveles de autoridad menores a dicho objeto o recurso.

Esta propiedad es muy útil cuando estamos clasificando transacciones que ya llevan implícitas las operaciones que se pueden realizar con los datos (update, delete, etc.). El nivel de utilidad marcará el nivel de ejecución del recurso en cuestión.

Modelo de Control de Accesos por «Roles» o por «Papeles en la organización»

Los investigadores de seguridad han comprobado que muchos requerimientos prácticos de control de accesos no están cubiertos por los modelos discrecionales y obligatorias clásicas.

Claramente y repasando un poco la historia de la seguridad los modelos obligatorios se han creado a partir de ambientes rígidos y jerarquizados, como puede ser el entorno militar. En cambio, los modelos discrecionales se han creado a partir de requerimientos cooperativos y a la vez autónomos, como son los entornos de investigación o académicos.

Un punto importante es que ningún de estos modelos satisface las necesidades de la mayoría de las empresas comerciales.

El modelo basado en «roles» regulan el acceso de los usuarios a la información en base a las actividades que ejecutan los usuarios en el la organización y la identificación de los «roles» en el sistema. Un «rol» puede ser definido como un conjunto de acciones y responsabilidades asociadas con una actividad del trabajo en particular. Por lo tanto, en vez de especificar todos los accesos que puede tener un usuario, las autorizaciones sobre objetos son especificadas para «roles». A los usuarios se les da autorización para adoptar «roles». Un estudio del NIST confirma que los «roles» son un planteamiento útil para muchas organizaciones comerciales y gubernamentales y sobre todo el único valido para entornos complejos (arquitectura cliente/servidos con entornos heterogéneos)

El enfoque basado en roles tiene las siguientes ventajas:

- **Gestión de Autorizaciones.** Las políticas basadas en roles se benefician de independencia lógica en la especificación de autorizaciones de usuario, dividiendo esta tarea en dos: asignar los usuarios a roles

y asignar los derechos de acceso de objetos a roles. Esto simplifica la gestión de la seguridad.

- **Roles Jerárquicos.** En muchas aplicaciones existe una jerarquía natural de roles, basada en los principios de generalización y especificación. Por ejemplo, los roles de un técnico de hardware y software son especializaciones del rol de técnico. Un usuario asignado al rol de técnico de software también heredará los privilegios y permisos asignados al rol general de técnico. Los roles jerárquicos simplifican más la gestión de autorizaciones.
- **El menor Privilegio.** Los roles permiten a un usuario conectarse con el mínimo privilegio necesario para la tarea que está realizando. Los usuarios con privilegios poderosos no necesitan ejercitarlos a menos que esos privilegios sean necesarios. Esto minimiza el peligro de daños debidos a errores involuntarios o de intrusos enmascarados como usuarios legítimos.
- **Segregación de Funciones.** La segregación de funciones se refiere al principio de que a ningún usuario debe dársele los privilegios suficientes para hacer mal uso del sistema. Por ejemplo, la persona que autoriza el pago de un cheque no debe ser la misma que lo prepara. La segregación de funciones puede reforzarse estáticamente (definiendo roles contradictorios, que no pueden ser ejecutados por el mismo usuario) o dinámicamente (reforzando el control en el momento del acceso).
- **Clases de Objetos.** Las políticas basadas en roles suministran una clasificación de los usuarios de acuerdo a las actividades que ejecutan. Análogamente, puede realizarse una clasificación para los recursos u objetos. Estos pueden clasificarse por tipo (cartas, manuales, etc.), o por área de aplicación (cartas comerciales, cartas promocionales, etc.). Las autorizaciones de acceso por roles debe realizarse en base a clases de recursos u objetos, no a recursos u objetos específicos.

La última pata de la silla del control de accesos es la administración de autorizaciones. Las políticas administrativas determinan quién está autorizado a modificar los accesos permitidos. Este es uno de los aspectos más importantes y menos entendidos de los controles de acceso.

En los controles de acceso obligatorios, los accesos permitidos están determinados en base a la clasificación de seguridad de usuarios y recursos u objetos. El administrador de seguridad asigna niveles de seguridad

a los usuarios. Los niveles de seguridad de recursos u objetos son determinados por el sistema en base a los niveles de los usuarios que los crean. Normalmente, el administrador de seguridad es el único que puede cambiar los niveles de seguridad de sujetos u objetos.

Los controles de acceso discrecionales permiten gran variedad de políticas administrativas:

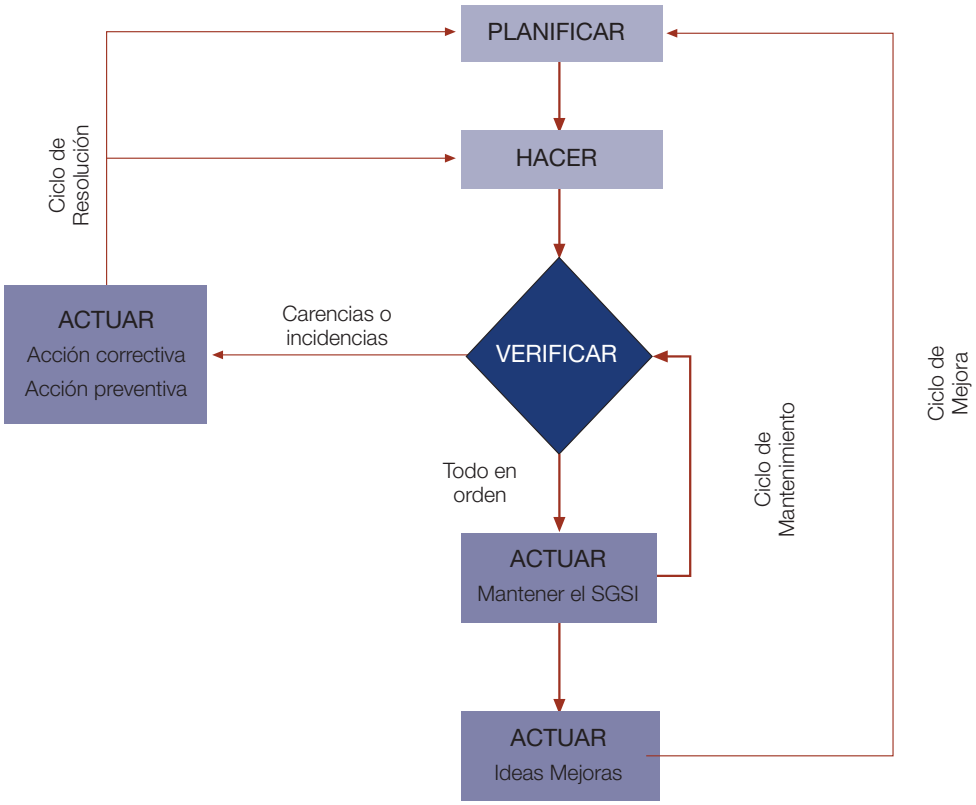
- **Centralizada.** Un único usuario (o grupo) puede dar o restringir acceso a los usuarios.
- **Jerárquica.** Un autorizador central es responsable de asignar responsabilidades a otros administradores. Los administradores pueden dar o restringir acceso a los usuarios del sistema.
- **Cooperativo.** Las autorizaciones especiales sobre recursos específicos no puede ser otorgadas por un solo autorizador, sino que deben realizarlo varios.
- **Propiedad.** Un usuario es considerado propietario de los recursos u objetos que crea. El propietario puede otorgar o restringir el acceso a ese objeto a otros usuarios.
- **Descentralizada.** En la administración descentralizada el propietario de un objeto puede otorgar a otros usuarios el privilegio de administrar autorizaciones sobre el recurso u objeto.

Los accesos basados en roles tienen una variedad similar de políticas administrativas. En este caso, los roles también pueden emplearse para gestionar y controlar los mecanismos administrativos.

La delegación de autoridad administrativa es un área importante en el que los controles de acceso existentes son deficientes. En grandes sistemas distribuidos la administración centralizada de derechos de acceso es inviable. Algunos sistemas permiten la autoridad de administración para un conjunto de recursos u objetos delegado por el administrador central de seguridad a otros administradores de seguridad. El control de estos últimos puede administrarse centralmente, pero pueden tener una autonomía considerable en su área.

Para finalizar con el ISO, explicar que todo el modelo se basa como en calidad, en un proceso de mejora continúa PDCA: Planificar, Implantar, Revisar y Mejorar, tal y como se muestran en las siguientes figuras:

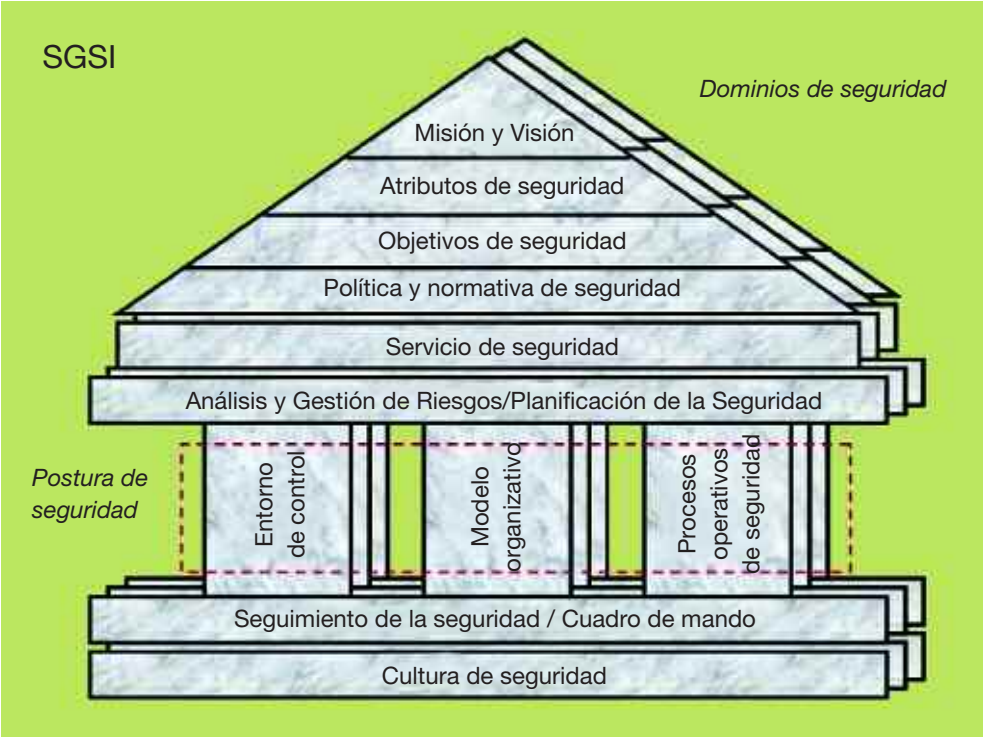
Modelo PDCA: Planificar, Hacer, Verificar y Actuar



Modelo PDCA (Planificar, Hacer, Verificar y Actuar)

3.3._Otro Modelo de Seguridad

Uno de los problemas que me he encontrado en la implantación de al seguridad de la información en las organizaciones es la adopción de un modelo completo que recoja todos los puntos que hemos visto hasta el momento. Franz Hassmann, compañero y amigo, hemos desarrollado un modelo que persigue poder implantar y mantener la seguridad, de una manera lógica y comprensiva en las organizaciones, con un mapa de ruta que permita, ir pasos a paso, construyendo un sistema de gestión de la seguridad de la información. En la siguiente figura se muestra el modelo completo que iremos explicando paso a paso.



4_COMPONENTES DEL MODELO DE SEGURIDAD

Misión y Visión

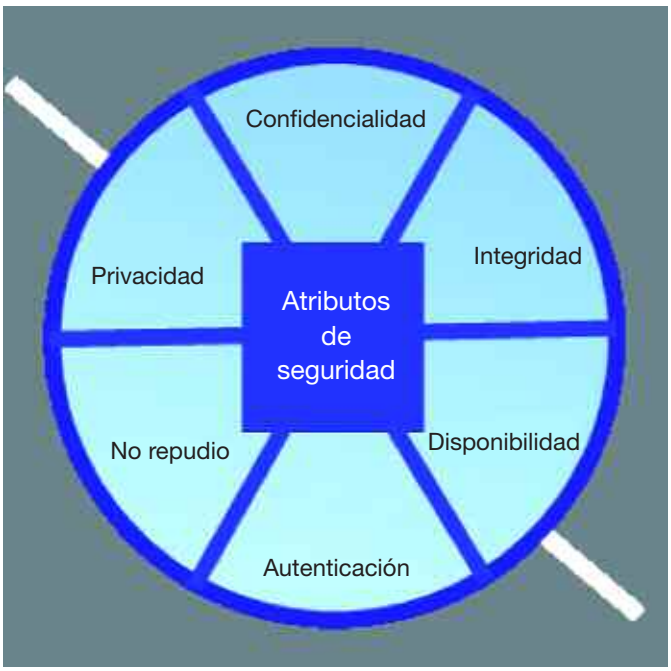
La misión y visión de la Organización de seguridad describen de forma clara y concisa cuál es la razón de ser de la misma en materia de seguridad y cómo se desea que la función ese encuentre posicionada en los próximos años. En base a las mismas se desarrollará el resto del mode-

lo, puesto que establece las prioridades y lo que es importante en materia de seguridad para el resto de componentes. Como ejemplo, lo comentado anteriormente, ¿dentro de la seguridad de la información está contenida la disponibilidad y continuidad? Es en la misión donde debe estar implícito cual es el ámbito de esta.

Dicha misión y visión debe estar adecuadamente alineada con la misión y visión de la estrategia de negocio y/o de sistemas de información con el fin de garantizar la contribución de valor de la seguridad a la Organización.

Atributos de seguridad

Los atributos de seguridad describen las propiedades, en términos de seguridad, que hay que considerar para garantizar una adecuada protección de los activos de información en base a las necesidades de seguridad y el tipo de sector al que pertenece la Organización. Dichos atributos deben ser acordes a la misión y visión de seguridad descritos anteriormente.



Dominios de seguridad

Los dominios de seguridad ámbitos de los sistemas de información donde las necesidades y atributos de seguridad son análogos. De esta

forma, cada uno de los dominios de seguridad estará constituido por entornos de la organización o agrupaciones de usuarios o sistemas de información y elementos de seguridad los cuales, tienen las mismas «necesidades» de seguridad, los mismos atributos y, por tanto, es posible aplicar los mismos objetivos y mecanismos de seguridad.

- Objetivos de seguridad

Una vez definidos de forma concisa la misión y visión de la Organización, así como los atributos de seguridad necesarios para el modelo, es necesario plasmar en forma de objetivos de seguridad de forma explícita y concreta que desea alcanzar la Organización a largo plazo para cada uno de los dominios de Seguridad definidos previamente. Dichos objetivos marcarán las directrices y las actuaciones que se lleven a cabo en el corto y medio plazo, y serán la base del cuadro de mando con el fin de ser capaces de valorar si los mismos están siendo alcanzados de forma continua y objetiva. Los objetivos de seguridad no son los objetivos de control ISO, deben ser objetivos concisos y si es posible cuantificables, como por ejemplo, tener un implantado un sistema de autorización basado en roles en la capa de aplicación, los usuarios con privilegios a la capa de infraestructura de información deberán poseer mecanismos de autenticación fuerte para acceder a las utilidades de administración de la misma, etc.

Política y Normativa de Seguridad

El Cuerpo Normativo de Seguridad está constituido por la Política de Seguridad, Normativa de Seguridad de primer nivel, Normativa de seguridad de segundo nivel (Guías y Estándares de Seguridad) y Procedimientos generales y específicos de seguridad. Dicho cuerpo normativo marca las directrices en materia de seguridad y conforme a los objetivos de seguridad definidos previamente.

La composición del cuerpo normativo de seguridad tiene en consideración no sólo el público objetivo al que está dirigido en la Organización, sino que su diseño modular permite llevar a cabo un desarrollo paulatino del mismo y garantizar su ciclo de revisión del mismo con eficiencia y eficacia.

La Política de Seguridad define, a nivel estratégico, las principales directrices y líneas de actuación en seguridad de forma muy general, estableciendo así los principios, objetivos y responsabilidades y marco de actuación por la Dirección de la Organización. Un punto clave de la política, que afectará

únicamente a los niveles jerárquicos inferiores de la persona que la firma. Es por esto que es mejor introducir un párrafo sobre seguridad de la información en la política de calidad y medioambiente de la compañía y firmada por la más alta jerarquía de la organización, que el gran documento de política de seguridad firmada or el responsable de organización y sistemas.

La Normativa de primer nivel desarrolla y detalla, a nivel táctico, los principios de seguridad plasmados en forma de Política. Se desarrollan tantas normativas de primer nivel como aspectos de seguridad existentes en la misma, y generalmente se agrupan por ámbitos de actuación (seguridad física, seguridad en recursos humanos, seguridad de operaciones y comunicaciones, gestión de la continuidad de negocio, etc.). Una vez desarrollada dicha normativa, se lleva a cabo el desarrollo de la Normativa de Seguridad de segundo nivel, donde se detalla de forma más concisa y se profundiza cada uno de los ámbitos en forma de Guías y Estándares de seguridad, los cuales conformarán el marco de desarrollo de los Procedimientos de seguridad.

Los Procedimientos de seguridad, ya sean de carácter general o específico, son la base de la operación de seguridad en día a día. De esta forma su desarrollo formal permite, a nivel operativo, definir claramente el cómo de la seguridad para los individuos de la Organización y garantiza que las acciones sean repetibles y ejecutadas de forma adecuada desde el punto de vista de la calidad de lo que se hace.

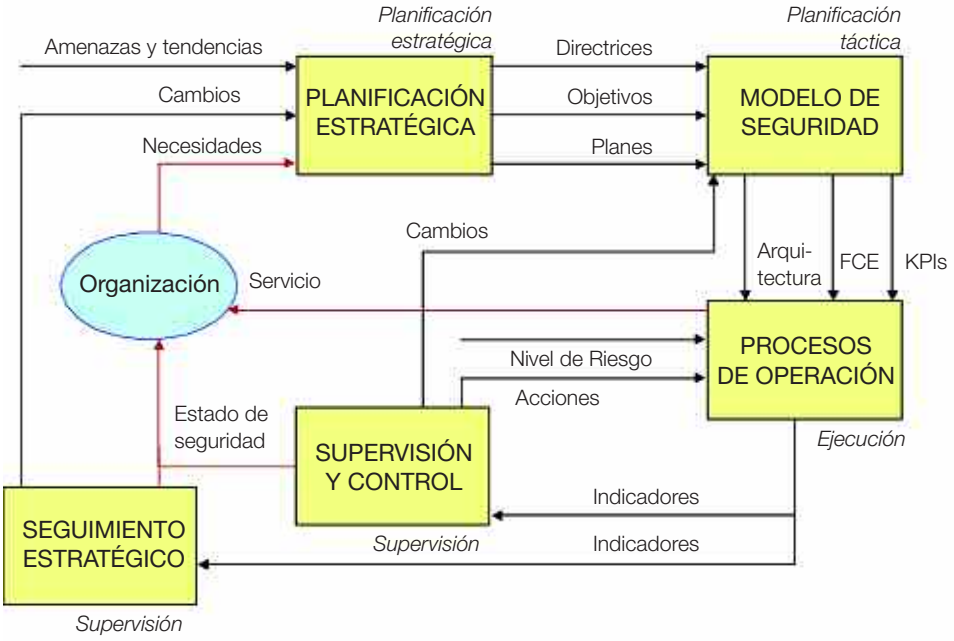
Todos los procedimientos deberán contar con una descripción detallada del resultado de la ejecución del mismo a modo de Registro Documental. Dichos registros permitirán garantizar que la seguridad se está llevando a cabo adecuadamente frente a terceras partes independientes y auditores, ya que son la piedra angular de las certificaciones de seguridad basadas en estándares internacionales como el ISO/IEC 27001:2005, que certifica el Sistema de Gestión de la Seguridad de la Información (SGSI) de una Organización.

Servicio de Seguridad

El Servicio de Seguridad se puede definir como el «Conjunto de actividades, conocimiento y recursos técnicos y humanos que se ponen a disposición de la Organización con el fin de satisfacer sus necesidades en el ámbito de la seguridad; y que se articulan mediante Procesos de Planificación, Operación y Supervisión.».

Durante mucho tiempo se ha dicho que «la seguridad es un proceso», si bien a día de hoy ha evolucionado suficientemente para que podamos decir que la seguridad es un ***servicio*** más que se pone a disposición a los clientes internos y externos de la Organización.

Dicho servicio está sustentado por tres grandes macroprocesos de seguridad: Planificación, Operación y Seguimiento (Seguimiento estratégico - Supervisión y Control). Cada uno de estos tres macroprocesos se puede desglosar en procesos de carácter específico en base a la Postura de seguridad que adopta una Organización, aspecto que se describirá posteriormente con mayor nivel de detalle.



De esta forma, es posible que algunos de las actividades pertenecientes a procesos de seguridad de Operación, como por ejemplo la administración de elementos técnicos de seguridad, puedan ser delegados en las actividades de otras áreas y departamentos pertenecientes al área de Sistemas de Información.

Análisis de Seguridad / Planificación de Seguridad

Este componente del modelo, cuya actividad se articula mediante los macroprocesos de Planificación, tiene como fin último la planificación concreta de las actuaciones de seguridad con el fin de que las mismas

se encuentren correctamente alineadas con todos los elementos anteriores del modelo de seguridad.

En función de las preferencias y nivel de madurez de cada Organización el ejercicio de análisis para llevar a cabo dicha planificación se puede llevar a cabo de forma más o menos formal.

Típicamente dicho análisis se lleva a cabo mediante un Análisis de Riesgos, en el cual se determinan los principales riesgos, en términos de probabilidad e impacto, a los que están expuestos los principales activos de información de la Organización. Contando con el resultado del análisis se define un Plan de Gestión del Riesgo según el cual se decide, para cada uno de los riesgos, si éste se Transfiere, se Evita, se Asume o se Mitiga. En este último caso también será necesario definir aquellos mecanismos, controles técnicos o procedimentales que es necesario implantar para que la Organización cuente con un nivel de riesgo residual con el que se sienta confortable. Dichos elementos conformarán lo que se entiende por Postura de Seguridad, que se detallará posteriormente.

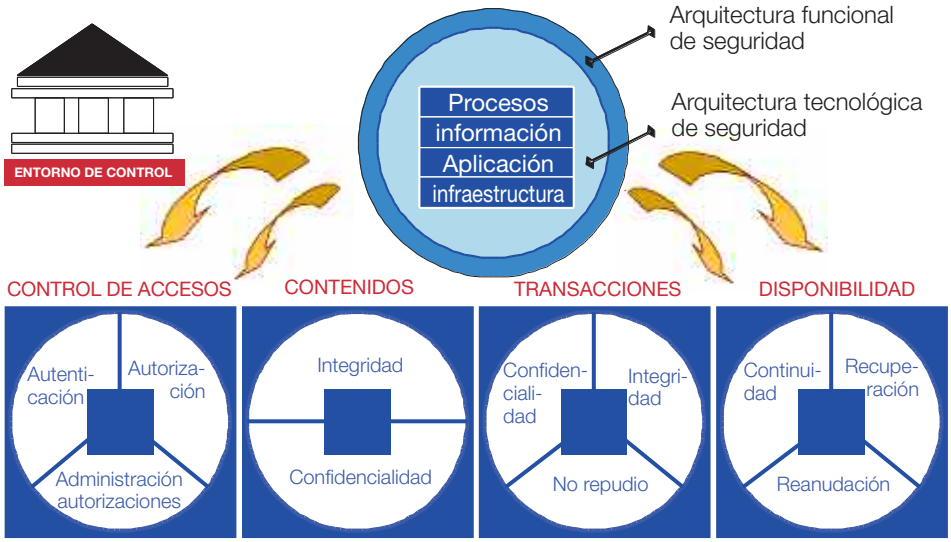
Una vez determinadas las actuaciones de seguridad concretas que es necesario acometer según en análisis llevado a cabo (ya sea formal o informalmente), también será necesario definir un Plan de Acción debidamente priorizado con las estimaciones en términos de tiempo, esfuerzo y coste asociadas a cada una de las iniciativas definidas, momento en el que finaliza la fase de Planificación.

Postura de Seguridad

La Postura de seguridad de una Organización se puede definir como «el conjunto de iniciativas, procesos y actividades de seguridad que se llevan a cabo en la Organización con el fin de alcanzar los objetivos de seguridad planificados y que tienen como referencia la misión, visión y valores vigentes».

Dicha la postura de seguridad de una organización estará formada por tres componentes estrechamente relacionados entre sí, y que determinan la gestión y operativa diaria de la seguridad en la Organización. Si bien se describen de forma independiente a continuación, es importante resaltar la definición de cada uno de estos tres pilares no es posible abordarla de forma independiente y aislada de los demás con el fin de garantizar la coherencia y equilibrio de la Postura de Seguridad.

El entorno de control



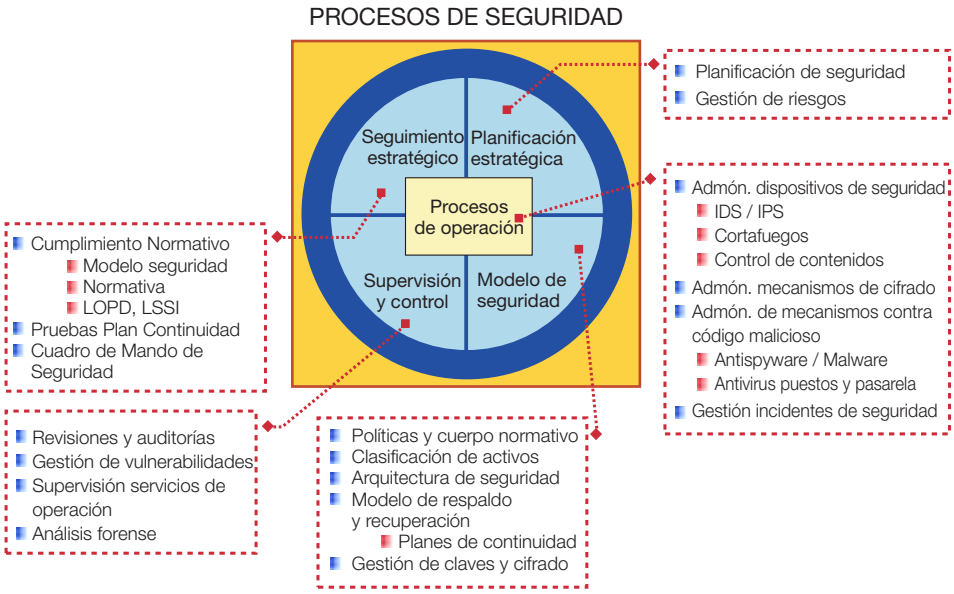
Para cada uno de los elementos que constituyen los sistemas de información de la Organización (procesos, información, aplicaciones e infrestructura tecnológica) es necesario definir, diseñar e implantar los mecanismos concretos de seguridad, tanto técnicos como procedimentales, para garantizar los objetivos de seguridad definidos para el Control de Accesos, Contenidos (información estática), Transacciones (información dinámica) y Disponibilidad.

Pero quizá lo más importante en este elemento del modelo es que dichos controles han de ser definidos de forma coherente y acorde a una visión global con el fin de que den soporte a la Arquitectura funcional y técnica de seguridad definida, de forma que todos los elementos estén correctamente interrelacionados entre sí y permita su evolución en el tiempo en términos de escalabilidad y optimización de costes, muchos de los cuales son ocultos (costes de formación, costes de mantenimiento y costes de administración).

Los procesos de operación

Como ya se ha descrito anteriormente, este grupo de procesos son los permiten llevar a cabo la gestión y operación del entorno de control definido anteriormente y son los que hacen posible que la seguridad de la Organización funcione en el día a día.

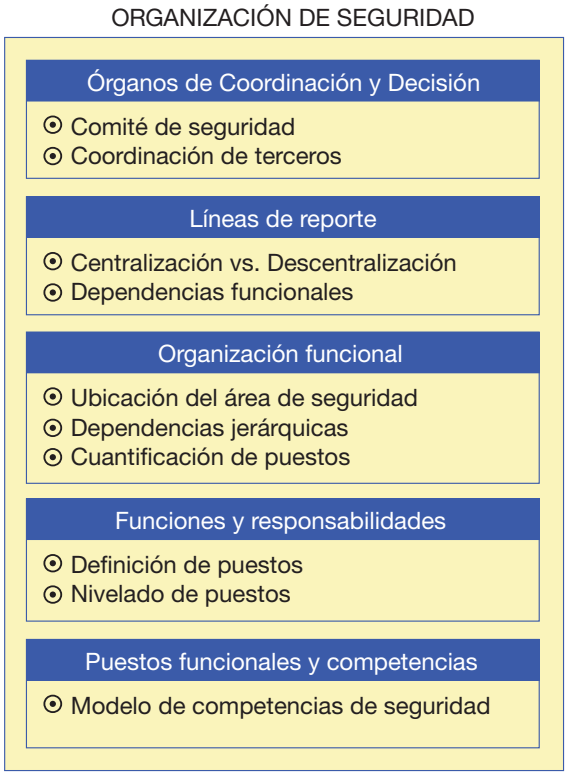
En función del entorno de control y del modelo organizativo adoptado (centralización/descentralización/mixto) cada Organización tendrá unos procesos operativos u otros adecuados a sus necesidades, si bien a continuación se desglosan, a modo de ejemplo, los principales procesos operativos concretos aplicables a una gran cantidad de casuísticas y organizaciones.



El Modelo organizativo

Para finalizar con la Postura de Seguridad, el Modelo organizativo tiene como fin de correcta definición la estructura organizativa y de los mecanismos de coordinación y reporte de la función de seguridad en una Organización.

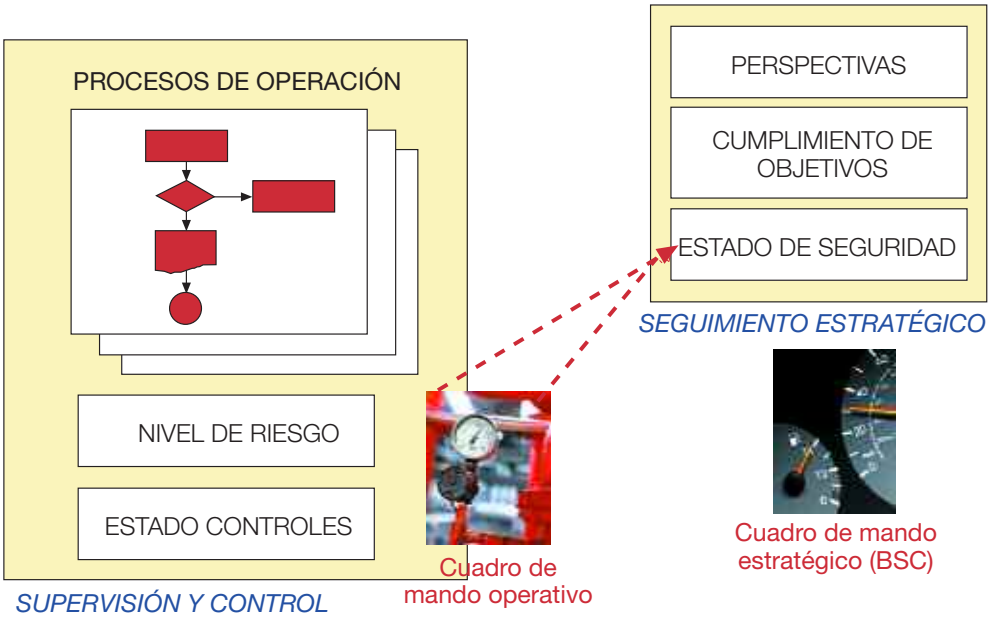
Si bien la estructura de seguridad de una Organización de tamaño medio o pequeño suele ser bastante sencilla, es necesario llevar a cabo una correcta definición de los siguientes aspectos que es necesario tener en consideración:



Seguimiento / Cuadro de Mando

Una vez que el Modelo de Seguridad está definido y desarrollado en la Organización, será necesario garantizar la adecuada supervisión y evolución de todo lo descrito anteriormente con el fin de garantizar el cumplimiento de los objetivos de seguridad definidos y convertir en realidad la misión y visión de la función de seguridad dentro de la Organización.

Según se describía anteriormente, el macroproceso de Seguimiento se desglosaba en dos grandes ámbitos: Supervisión y Control y Seguimiento estratégico. Por ello es necesario mantener un mecanismo de medición y seguimiento en el corto plazo (cuadro de mando operativo) y otro que permita la visión a medio y largo plazo (cuadro de mando estratégico - Balanced scorecard) de forma que el primero alimente y de soporte al segundo, tal y como se esquematiza en la siguiente figura:



Cultura de Seguridad

El último de los elementos del Modelo de Seguridad, y que constituye la base de toda la pirámide, es la Cultura de Seguridad. De hecho, si bien es conocido el dicho «las personas son el eslabón más débil de la seguridad», muchos de las vulnerabilidades y riesgos que se manifiestan en las Organizaciones provienen de ataques de ingeniería social y fallos no intencionados de seguridad por una formación y unas nociones generales de seguridad escasas.

En este sentido es imperativa la ejecución de programas de sensibilización, concienciación y divulgación de seguridad, así como acciones formativas específicas en función del colectivo específico al que se dirijan dichas actuaciones, como se representó en la figura 7:

- La sensibilización está orientada a los niveles estratégicos y tácticos de la Organización y tiene como meta el promover el uso de la seguridad para convertirla en un hábito, generando principalmente actitudes.
- La concienciación generalmente se dirige a los niveles tácticos y tiene como fin la potenciación de habilidades, es decir, en promover el saber hacer.
- La divulgación, que suele orientarse a colectivos operativos con mayor tamaño y cuya principal misión es la difusión de conocimientos y saber.

- Finalmente contamos con la formación, que al ser de carácter específico, suele ser un complemento a las anteriores y debe estar muy orientada a las necesidades concretas del uso de mecanismos y directrices de seguridad en la operativa diaria para el desempeño de las funciones del personal al que se dirige.

A la hora de abordar el diseño, desarrollo y la implantación exitosa de un programa de estas características los factores fundamentales son tener presente una adecuada segmentación del público, adecuar los objetivos concretos del programa para colectivo y la selección y uso de los canales de comunicación más eficaces para cada uno de ellos. Sólo de esta forma se logrará inculcar la cultura de seguridad, base de todo el modelo, en la cultura y valores vigentes en la Organización.

5_PAYMENT CARD INDUSTRY DATA SECURITY STANDARD (PCI DSS)

Como ya indicamos en el apartado 1, con el aumento de fraude electrónico y el impacto que ocasiona en la imagen de las compañías, hace dos años Visa y Mastercard desarrollaron el PCI (Payment Card Industry) para imponer un estándar de seguridad para la protección de los datos de las tarjetas de crédito. Desde entonces American Express, Diners Club Internacional, Discover Bank, and JCB International Credit Card han recomendado la implantación del mismo en sus clientes.

En Enero de 2005, VISA y Mastercard obligaron a los comerciantes y los proveedores de servicios que procesaban y almacenaban la información del titular de su tarjeta, que se certificaran en el PCI Data Security Standard. El estándar no fue aceptado por toda la industria de medios de pagos y el nivel de certificación era muy bajo, debido entre otras cuestiones a que las consecuencias de no adherirse a esta certificación estaban suficientemente definidas. Con un cambio de estrategia de las compañías de tarjetas de crédito que empezaron a amenazar a sus clientes con acciones muy severas, entre las que se incluían el pago de multas la perdida de prestaciones que tenían por el hecho de utilizar sus marcas. Además, obligaron a que los comerciantes y proveedores de servicio, fuesen los responsables de la seguridad de los datos del titular de tarjeta y a hacerse cargo de cualquier daño que pudiera ocurrir como

resultado de la explotación de alguna vulnerabilidad de la seguridad de los datos por el incumplimiento del PCI.

PCI detalla doce requisitos principales y requisitos secundarios de seguridad, previstos para asegurar, durante el proceso de transmisión, la información del titular de tarjeta.

Así mismo, estos requisitos proporcionan líneas para desarrollar y mantener los sistemas de información que procesan y almacenan los datos del titular de tarjeta. Estos requisitos se basan en gran parte en el ISO 17799.

PCI requiere a las empresas que van a realizar parte de sus transacciones mediante el uso de tarjetas de créditos a:

A construir y mantener una red segura

1. Instalar y mantener los cortafuegos (firewalls) configurados para proteger la información.
2. No utilizar los parámetros de seguridad que vienen configurados por defecto en los equipos.

Proteger los datos de los usuarios que utilizan la tarjeta de crédito

3. Proteger la información almacenada.
4. Cifrar la transmisión de la información sensible cuando esta es trasportada en redes públicas.

Mantener un programa de gestión de vulnerabilidades

5. Utilizar y mantener actualizado software anti-virus.
6. Desarrollar y mantener sistemas y aplicaciones seguras.

Implementar medidas para un control de acceso fuerte

7. Restringir el acceso a la información sensible al usuario y dejarle acceder sólo a aquella información que necesite.
8. Asignar un identificador único a cada persona que accede al sistema.
9. Restringir físicamente el acceso a los datos de los usuarios de las tarjetas.

Monitorizar y probar regularmente la red

10. Rastrear y monitorizar todos los accesos que se producen a los recursos de la red y los sistemas donde se tiene almacenados la información del usuario de la tarjeta.

11. Probar regularmente los sistemas y procesos de seguridad de seguridad.

Mantener una política de seguridad de la información

12. Crear y actualizar una política que trate sobre la seguridad de la información.

Para cada uno de los seis requerimientos anteriores se definen 1 varias recomendaciones. Al final se tienen 170 controles detallados para el proceso, almacenamiento, transmisión de los datos que contiene una tarjeta de crédito.

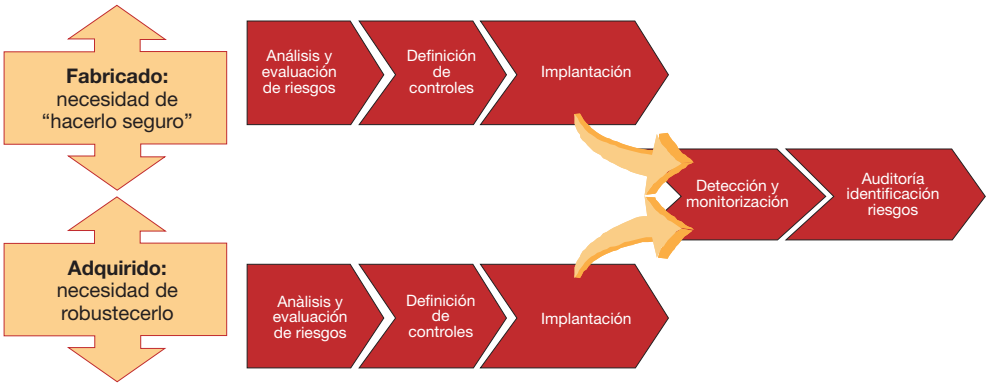
Aunque el PCI Security Standards Council es el responsable de desarrollar y mantener el estándar PCI, las compañías de tarjetas de crédito están definiendo el grado de implantación del mismo. Visa ha informado del grado de implantación de la PCI entre sus comerciantes, sólo el 36% de los comerciantes de nivel 1 (aquellos que procesan más de 6 millones de transacciones con tarjeta de crédito al año) y un 15% de los comerciantes de nivel 2 (aquellos que procesan entre 1 y 6 millones de transacciones al año).

Inicialmente Visa se esta centrando en los comerciantes de nivel 1 y nivel 2, porque son los que agrupan el núcleo principal de transacciones con VISA.

El porcentaje de implantación para el resto de comerciantes, los que procesan menos de 1 millón de transacciones al año) se estima por debajo de un 25%.

6_SEGURIDAD EN EL CICLO VIDA DE DESARROLLO

Uno de los puntos en los que incido y que creo que es fundamental es responder a esta pregunta ¿en que proceso puedo implantar todos los componentes de seguridad de una forma lógica y comprensiva? Creo que en el ciclo de vida de aplicaciones, ya que, es en este ciclo donde para lograr construir y mantener por completo todo el entorno tecnológico que enmarca un producto o servicio, debe aplicarse el ciclo de gestión de la seguridad tanto para los desarrollos fabricados a medida como a los productos y componentes adquiridos:



Actualmente las Organizaciones están bastante concienciadas de la necesidad de aplicar un ciclo de gestión de la seguridad a los productos y componentes adquiridos, así como a los servicios que se encuentran en producción.

Sin embargo no se tiene la misma consideración con los productos y servicios fabricados y desarrollados a medida, por lo que la seguridad no se suele contemplar en los ciclos de vida de desarrollo.

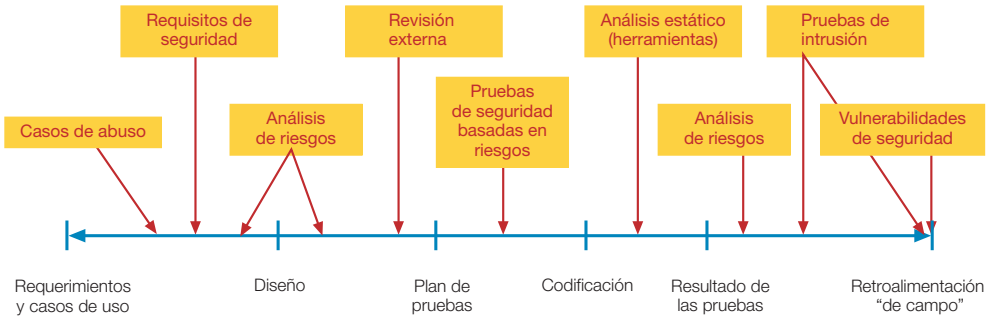
Esta falta de sensibilidad conlleva la siguiente problemática:

- El time-to-market de nuevos productos y servicios es cada vez más reducido, lo que deriva en una penalización de su grado de seguridad.
- La mayoría de los ataques con éxito se realizan explotando vulnerabilidades y fallos de seguridad en las aplicaciones y debido a la falta de aplicación de buenas prácticas de diseño y codificación.
- Es mucho más complicado y costoso hacer segura una aplicación ya desarrollada, que contemplar los requisitos de seguridad desde las fases iniciales del desarrollo.

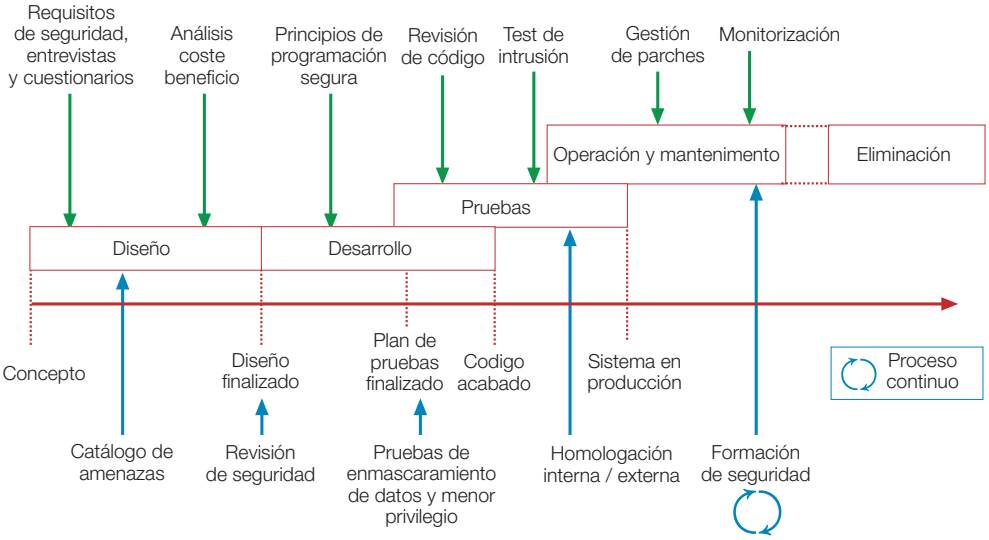
De esta forma, con el mitigar los riesgos y la solución a los problemas anteriores es imprescindible integrar la seguridad en el ciclo de vida de desarrollo de los productos y servicios de la Organización.

De reciente publicación, el principal marco de referencia en el ámbito del desarrollo seguro de aplicaciones y servicios se recoge en el SSDLC (Secure Software Development Life Cycle), en el cual se complementan las actividades llevadas a cabo por las fases habituales de ciclo de vida de desarrollo de software con actividades y tareas de carácter específico de seguridad, optimizando así la eficacia de la misma y obteniendo grandes

beneficios en términos de reducción de costes derivados del mantenimiento correctivo que necesitaría una aplicación una vez que requiere la introducción de medidas de seguridad una vez que ya está en producción.



A continuación, a modo ilustrativo, se describen las fases de desarrollo y las actividades y tareas de seguridad llevadas a cabo en el ciclo de vida tradicional de un servicio o aplicación.



Desde el punto de vista de su puesta en práctica, cuando se implanta una metodología de desarrollo seguro de servicios y aplicaciones en una Organización el principal problema al que nos exponemos son la formalización y adaptación del modelo «habitual» de desarrollo instaurado, por lo que el proceso de gestión del cambio se convierte en un factor crucial con el fin de minimizar la resistencia al cambio que generalmente nos encontramos con las áreas y departamentos de Desarrollo, ya sean internos o externos.

Sin embargo, una vez superados estos obstáculos, el retorno de la inversión en términos de «tranquilidad» y reducción de costes derivados del mantenimiento correctivo e incidentes de seguridad se vuelve un elemento a tener en consideración, pues en la actualidad la mayoría de las vulnerabilidades de seguridad (y las más preocupantes) se identifican y explotan a nivel de aplicación y no en elementos tecnológicos de la plataforma e infraestructura técnica de los sistemas de información.

Legislación y derecho aplicable al negocio en la red

Ignacio Alamillo
Director d'assessorament i recerca de la Agència Catalana de Certificació (CATCert)

1_EL CUMPLIMIENTO LEGAL Y DE LA SEGURIDAD DE LA INFORMACIÓN

Los aspectos legales juegan un papel cada vez más importante en la seguridad de la información, de forma pareja a la relevancia que presentan en relación con la gestión del negocio.

Diversos factores han contribuido a este protagonismo de las cuestiones jurídicas, entre los que debe considerarse la aparición, relativamente reciente, de normativa legal que regula de forma específica la seguridad de la información, en especial cuando se trata de información personal, información propiedad del sector público o que afecta a las denominadas infraestructuras críticas y a la seguridad nacional.

De esta forma se reconoce en normas de mejores prácticas en la gestión de la seguridad de la información, como ISO 17799:2005, que dedica al cumplimiento legal la sección 15.1 de sus recomendaciones.

Dicha sección establece como objetivo de control el «evitar infracciones de cualesquiera obligaciones legales, reglamentarias, administrativas o contractuales, así como de cualquier requisito de seguridad», partiendo de la consideración de que el diseño, la operación, el uso y la gestión de los sistemas de información puede encontrarse (y de hecho, suele ser el caso habitual) sujeto al cumplimiento de regulaciones jurídicas.

La norma ISO 17799:2005 identifica una serie de controles habituales, orientados al cumplimiento legal y de la seguridad de la información:

- Identificación de la legislación aplicable.
- Cumplimiento con los derechos de propiedad intelectual e industrial de terceros.
- Protección de los ficheros y archivos de la organización.
- Protección de los datos de carácter personal.

- Prevención del abuso de los sistemas de información.
- Uso de los controles criptográficos, incluyendo la firma electrónica y el cifrado de la información.

Dada la naturaleza de la norma internacional ISO 17799:2005, en este caso recopilando las mejores prácticas en materia de seguridad, cabe completar los controles que propone y adaptarlos a la práctica de cada Estado y cada tipo de organización, realizando una asesoría continua del grado de cumplimiento legal y gestionando los riesgos jurídicos correspondientes.

En España la normativa general sobre seguridad de la información se ha centrado en la protección de los datos de carácter personal, en un primer momento, y en la promoción de la identidad digital y la firma electrónica, más recientemente, cuestiones ambas íntimamente interrelacionadas.

De forma más particular, se han ido producido normas más concretas relativas a la seguridad de la información, como la regulación de la identificación e información mínimas en Internet de los prestadores de servicios de la sociedad de la información, el establecimiento de fuertes restricciones a actividades como las comunicaciones comerciales no solicitadas (SPAM) y de obligaciones iniciales de conservación de documentos electrónicos originales.

2_LA SEGURIDAD EN LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

Sin duda alguna, el motor que legalmente ha impulsado la adopción de medidas de seguridad en los sistemas de información generales[1], especialmente en el sector privado, ha sido la normativa de protección de datos de carácter personal.

Nuestra vigente Ley Orgánica 15/1999, de 13 de diciembre, establece el marco referencial para todo tratamiento de datos de carácter personal, mientras que el Real Decreto 994/1999, de 11 de junio[2], establece el

1. No cabe decir lo mismo de los sistemas de información clasificada, en especial en el ámbito de la seguridad nacional y de las infraestructuras críticas de información, en las que tradicionalmente ya venían aplicándose elevadas medidas de seguridad.
2. Se encuentra, en el momento de redacción de este texto, pendiente de aprobación y publicación el denominado Nuevo Reglamento de Medidas de Seguridad, que actualiza la normativa reglamentaria actualmente vigente.

conjunto mínimo de medidas de seguridad aplicables a los sistemas de información que contienen datos personales, y que procede presentar a continuación.

Conviene indicar que las medidas de seguridad exigibles a los sistemas de información son diferentes en función de la categoría de datos personales tratados, diferenciándose en tres niveles, de acuerdo con el artículo 4 del reglamento, que establece lo siguiente:

«1. Todos los ficheros que contengan datos de carácter personal deberán adoptar las medidas de seguridad calificadas como de nivel básico.

«2. Los ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros y aquellos ficheros cuyo funcionamiento se rija por el artículo 28 de la Ley Orgánica 5/1992, deberán reunir, además de las medidas de nivel básico, las calificadas como de nivel medio.

«3. Los ficheros que contengan datos de ideología, religión, creencias, origen racial, salud o vida sexual así como los que contengan datos recabados para fines policiales sin consentimiento de las personas afectadas deberán reunir, además de las medidas de nivel básico y medio, las calificadas de nivel alto.

«4. Cuando los ficheros contengan un conjunto de datos de carácter personal suficientes que permitan obtener una evaluación de la personalidad del individuo deberán garantizar las medidas de nivel medio establecidas en los artículos 17, 18, 19 y 20.

«5. Cada uno de los niveles descritos anteriormente tienen la condición de mínimos exigibles, sin perjuicio de las disposiciones legales o reglamentarias específicas vigentes.»

2.1_Medidas de seguridad contempladas en el nivel básico

2.1.1_*El documento de seguridad*

El responsable del fichero debe elaborar e implantar la normativa de seguridad mediante un documento de obligado cumplimiento para el personal con acceso a los datos automatizados de carácter personal y a los sistemas de información.

Dicho documento deberá contener, como mínimo, los siguientes aspectos:

- Ámbito de aplicación del documento con especificación detallada de los recursos protegidos.
- Medidas, normas, procedimientos, reglas y estándares encaminados a garantizar el nivel de seguridad exigido por el Reglamento
- Funciones y obligaciones del personal.
- Estructura de los ficheros con datos de carácter personal y descripción de los sistemas de información que los tratan.
- Procedimiento de notificación, gestión y respuesta ante las incidencias.
- Los procedimientos de realización de copias de respaldo y de recuperación de los datos.

El documento deberá mantenerse en todo momento actualizado y deberá ser revisado siempre que se produzcan cambios relevantes en el sistema de información o en la organización del mismo.

El contenido del documento deberá adecuarse, en todo momento, a las disposiciones vigentes en materia de seguridad de los datos de carácter personal.

2.1.2_*Funciones y obligaciones del personal*

Las funciones y obligaciones de cada una de las personas con acceso a los datos de carácter personal y a los sistemas de información estarán claramente definidas y documentadas.

El responsable del fichero adoptará las medidas necesarias para que el personal conozca las normas de seguridad que afecten al desarrollo de sus funciones así como las consecuencias en que pudiera incurrir en caso de incumplimiento.

2.1.3_*Registro de incidencias*

Debe existir un procedimiento de notificación y gestión de incidencias, que deberá contener necesariamente un registro en el que se haga constar el tipo de incidencia, el momento en que se ha producido, la persona que realiza la notificación, a quién se le comunica y los efectos que se hubieran derivado de la misma.

2.1.4_*Identificación y autenticación, y control de acceso*

El responsable del fichero se encargará de que exista una relación actualizada de usuarios que tengan acceso autorizado al sistema de información y de establecer procedimientos de identificación y autenticación para dicho acceso.

Cuando el mecanismo de autenticación se base en la existencia de contraseñas existirá un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad. Las contraseñas se cambiarán con la periodicidad que se determine en el documento de seguridad y mientras estén vigentes se almacenarán de forma ininteligible.

Debe en este lugar indicarse que el nuevo reglamento de medidas de seguridad fomenta el empleo de los certificados electrónicos de firma electrónica para la función de identificación y autenticación.

Los usuarios tendrán acceso autorizado únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones.

El responsable del fichero establecerá mecanismos para evitar que un usuario pueda acceder a datos o recursos con derechos distintos de los autorizados.

Exclusivamente el personal autorizado para ello en el documento de seguridad podrá conceder, alterar o anular el acceso autorizado sobre los datos y recursos, conforme a los criterios establecidos por el responsable del fichero.

2.1.5_*Gestión de soportes, copias de respaldo y recuperación*

Los soportes informáticos que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados y almacenarse en un lugar con acceso restringido al personal autorizado para ello en el documento de seguridad.

La salida de soportes informáticos que contengan datos de carácter personal, fuera de los locales en los que esté ubicado el fichero, únicamente podrá ser autorizada, por el responsable del fichero.

El responsable de fichero se encargará de verificar la definición y correcta aplicación de los procedimientos de realización de copias de respaldo y de recuperación de los datos.

Los procedimientos establecidos para la realización de copias de respaldo y para la recuperación de los datos deberán garantizar su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción.

Deberán realizarse copias de respaldo, al menos semanalmente, salvo que en dicho periodo no se hubiera producido ninguna actualización de los datos.

2.2_Medidas de seguridad contempladas en el nivel medio

2.2.1_*Documento de seguridad. Responsable de seguridad*

El documento de seguridad deberá contener, además de lo dispuesto en el artículo 8 del reglamento, la identificación del responsable o responsables de seguridad, los controles periódicos que se deban realizar para verificar el cumplimiento de lo dispuesto en el propio documento y las medidas que sea necesario adoptar cuando un soporte vaya a ser desechado o reutilizado.

El responsable del fichero designará uno o varios responsables de seguridad encargados de coordinar y controlar las medidas definidas en el documento de seguridad. En ningún caso esta designación supone una delegación de la responsabilidad que corresponde al responsable del fichero de acuerdo con el reglamento.

2.2.2_*Auditoría*

Los sistemas de información e instalaciones de tratamiento de datos se someterán a una auditoría interna o externa, que verifique el cumplimiento del reglamento, de los procedimientos e instrucciones vigentes en materia de seguridad de datos, al menos, cada dos años.

El informe de auditoría deberá dictaminar sobre la adecuación de las medidas y controles con el reglamento, identificar sus deficiencias y proponer las medidas correctoras o complementarias necesarias.

Deberá, igualmente, incluir los datos, hechos y observaciones en que se basen los dictámenes alcanzados y recomendaciones propuestas.

Los informes de auditoría serán analizados por el responsable de seguridad competente, que elevará las conclusiones al responsable del fichero

para que adopte las medidas correctoras adecuadas y quedarán a disposición de la Agencia de Protección de Datos.

2.2.3_*Registro de incidencias*

En el registro al que se refiere el artículo 10 del reglamento deberán consignarse, además, los procedimientos realizados de recuperación de los datos, indicando la persona que ejecutó el proceso, los datos restaurados y, en su caso, qué datos ha sido necesario grabar manualmente en el proceso de recuperación.

Será necesaria la autorización por escrito del responsable del fichero para la ejecución de los procedimientos de recuperación de los datos.

2.2.4_*Identificación y autenticación. Control de acceso físico*

El responsable del fichero establecerá un mecanismo que permita la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información y la verificación de que está autorizado.

Se limitará la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información.

Exclusivamente el personal autorizado en el documento de seguridad podrá tener acceso a los locales donde se encuentren ubicados los sistemas de información con datos de carácter personal.

2.2.5_*Gestión de soportes*

Deberá establecerse un sistema de registro de entrada de soportes informáticos que permita, directa o indirectamente, conocer el tipo de soporte, la fecha y hora, el emisor, el número de soportes, el tipo de información que contienen, la forma de envío y la persona responsable de la recepción que deberá estar debidamente autorizada.

Igualmente, se dispondrá de un sistema de registro de salida de soportes informáticos que permita, directa o indirectamente, conocer el tipo de soporte, la fecha y hora, el destinatario, el número de soportes, el tipo de información que contienen, la forma de envío y la persona responsable de la entrega que deberá estar debidamente autorizada.

Cuando un soporte vaya a ser desechado o reutilizado, se adoptarán las medidas necesarias para impedir cualquier recuperación posterior de la información almacenada en él, previamente a que se proceda a su baja en el inventario.

Cuando los soportes vayan a salir fuera de los locales en que se encuentren ubicados los ficheros como consecuencia de operaciones de mantenimiento, se adoptarán las medidas necesarias para impedir cualquier recuperación indebida de la información almacenada en ellos.

2.2.6_*Pruebas con datos reales*

Las pruebas anteriores a la implantación o modificación de los sistemas de información que traten ficheros con datos de carácter personal no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente al tipo de fichero tratado.

2.3_Medidas de seguridad contempladas en el nivel alto

2.3.1_*Distribución de soportes*

La distribución de los soportes que contengan datos de carácter personal se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que dicha información no sea inteligible ni manipulada durante su transporte.

2.3.2_*Registro de accesos*

De cada acceso se guardarán, como mínimo, la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado.

En el caso de que el acceso haya sido autorizado, será preciso guardar la información que permita identificar el registro accedido.

Los mecanismos que permiten el registro de los datos detallados en los párrafos anteriores estarán bajo el control directo del responsable de seguridad sin que se deba permitir, en ningún caso, la desactivación de los mismos.

El período mínimo de conservación de los datos registrados será de dos años.

El responsable de seguridad competente se encargará de revisar periódicamente la información de control registrada y elaborará un informe de las revisiones realizadas y los problemas detectados al menos una vez al mes.

2.3.3_*Copias de respaldo y recuperación*

Deberá conservarse una copia de respaldo y de los procedimientos de recuperación de los datos en un lugar diferente de aquél en que se encuentren los equipos informáticos que los tratan cumpliendo en todo caso, las medidas de seguridad exigidas en este Reglamento.

2.3.4_*Empleo de redes de telecomunicaciones*

La transmisión de datos de carácter personal a través de redes de telecomunicaciones se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible

3_LA IDENTIDAD DIGITAL Y LA FIRMA ELECTRÓNICA

3.1_La identidad digital

Bajo la expresión «identidad digital» se han venido agrupando, de forma reciente, las técnicas que permiten a las personas y a las organizaciones identificarse y actuar en las redes, mediante mecanismos de autenticación de mayor o menor robustez.

En general, la identidad digital se construye empleando datos o atributos que nos diferencian de forma suficiente de otras personas o entidades, siempre dentro de un ámbito concreto, como por ejemplo el nombre y los apellidos, los diferentes números de identificación que se nos asignan desde organizaciones públicas o privadas (DNI, tarjeta sanitaria, otros...)

La identidad debe ser asignada de acuerdo con la legislación vigente, si bien puede ser acreditada mediante múltiples documentos, en función de las necesidades concretas.

De esta forma, mientras que la identidad personal y la condición de nacional se acreditan mediante el documento nacional de identidad, los extranjeros son también identificados mediante otros instrumentos. En el

ámbito corporativo, se emplean tarjetas de trabajadores frecuentemente, mientras que en las relaciones comerciales es frecuente disponer de diferentes tarjetas de identificación de cliente.

Por este motivo, hay que asumir que todos disponemos de diversas identidades parciales, a lo largo de nuestra vida, adecuadas a los diferentes roles y actividades que realizamos, variedad que, como no puede ser de otra forma, se ha proyectado a la identificación digital, en las redes de comunicaciones electrónicas.

Desde la perspectiva que interesa en este trabajo, hay que considerar que las organizaciones públicas y privadas han venido asignando mecanismos de identidad digital a su personal, y que cabe aplicar una serie de controles jurídicos a dicha actividad.

Adicionalmente, hay que considerar que hasta la fecha se han venido empleando, y se siguen empleando, nombres de usuario y contraseñas, aunque rápidamente se aprecia un avance de los sistemas basados en firma electrónica y certificados reconocidos, especialmente debido al incremento de la cultura de la seguridad y a la nueva regulación administrativa.

Junto a los mecanismos de identificación y autenticación directa, entre el usuario y la aplicación de la organización, debido al incremento de la complejidad de los modelos de relación entre usuarios y aplicaciones, dicho modelo ha presentado limitaciones que se tratan de superar con nuevas técnicas, y, en concreto, con la autenticación distribuida (y, por tanto, delegada) y la federación de la identidad, además de la firma electrónica ya vista.

En este sentido, la norma ISO 17799:2005 recomienda el establecimiento de las oportunas relaciones contractuales entre las personas identificadas y la organización, regulando el empleo de dicha identidad digital, y por supuesto cabe aplicar en toda su extensión la normativa de protección de datos de carácter personal anteriormente presentada.

3.2_La firma electrónica

La expresión «firma electrónica» se refiere a los mecanismos técnicos que, además de permitir identificarse y actuar en las redes, permite la producción de documentos originales y auténticos en forma electrónica,

así como la prestación del consentimiento y la producción de las oportunas evidencias documentales electrónicas.

De esta forma, cabe indicar que toda firma electrónica es una identidad digital, pero que no toda identidad digital permite firmar electrónicamente.

3.2.1_*La firma electrónica ordinaria*

El primer tipo de firma electrónica puede identificarse como «firma electrónica ordinaria», y, de acuerdo con el artículo 3.1 de la Ley 59/2003, es «el conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante».

Esta definición permite que todos los mecanismos técnicos de autenticación sean potencialmente considerados como la firma electrónica de una persona, dado que, de acuerdo con el artículo 3.9 de la Ley 59/2003 señala que «No se negarán efectos jurídicos de una firma electrónica que no reúna los requisitos de firma electrónica reconocida en relación con los datos a los que esté asociada por el mero hecho de presentarse en forma electrónica».

Es correcto pensar, en principio, en que todos los mecanismos de autenticación, como el número personal de identificación (PIN, en sus siglas en inglés) sirven como firma electrónica, y de hecho, en gran cantidad de contratos de acceso a servicios telemáticos, se establece que el PIN del usuario es la firma electrónica del usuario.

A pesar de que esta consideración es correcta, no elimina la realidad de las cosas, y esta realidad es que el PIN –al igual que sucede con los mecanismos de seguridad simétricos, en los que ambas partes conocen los datos para la autenticación– puede utilizarse para lograr una autenticación en el sentido de identificar a la entidad (en este caso, a la persona), pero difícilmente va a permitir una autenticación en el sentido de vincular un mensaje de datos con esa persona.

Por tanto, cabe indicar que la firma electrónica ordinaria es sencillamente un mecanismo de identidad digital, y que no resulta idóneo para la firma de documentos, de acuerdo con la propia dicción legal.

En particular, y aunque un PIN pueda calificarse de firma electrónica ordinaria, el propio sentido común nos indica que no puede ser en todos

los casos una firma equivalente a una firma manuscrita, porque no establece un vinculo con el firmante y el documento.

Este hecho tiene un impacto directo en la efectividad potencial de la firma electrónica ordinaria: porque la lectura correcta del artículo 3.9 de la Ley 59/2003 es que no se negarán efectos a la firma por esas circunstancias específicas, pero que sí se podrán negar efectos por otras circunstancias, como que la firma electrónica no pueda considerar suficientemente segura, o que no permita establecer un vínculo suficientemente fiable entre firmante y mensaje firmado.

En el caso del PIN, la ausencia de este vínculo es muy palpable: no hay operación objetiva que permita verificar que mensaje y firma corresponden el uno al otro, a diferencia de lo que sucede con una firma digital. Por el contrario, este vínculo es puramente arbitrario, establecido en un registro (*log*, en inglés) operado por el comercio, por ejemplo, que no tiene impedimento técnico alguno para inventarse transacciones del usuario, dado que la «firma» de la transacción es un número PIN que el comercio puede conocer perfectamente.

3.2.2_*La firma electrónica avanzada*

La firma electrónica avanzada es aquélla que cumple los siguientes requisitos (artículo 3.2 de la Ley 59/2003):

a) Permite identificar al firmante;

b) Permite detectar cualquier cambio ulterior de los datos firmados;

c) Está vinculada al firmante de manera única;

d) Está vinculada a los datos a que se refiere; y

e) Ha sido creada por medios que el firmante puede mantener bajo su exclusivo control.

La definición de firma electrónica avanzada se basa, por supuesto, en la definición de firma electrónica; es decir, los datos en forma electrónica anejos a otros datos electrónicos o asociados de manera lógica con ellos, utilizados como medio de autenticación (artículo 3.1 de la Ley 59/2003). Se trata de un tipo de firma electrónica de mayor seguridad y calidad, susceptible de recibir efectos jurídicos.

La firma electrónica avanzada es un concepto neutral desde un punto de vista tecnológico, que permite que diferentes tecnologías reciban equivalentes efectos jurídicos.

En la práctica actual, la tecnología más extendida en el campo de las firmas electrónicas es la tecnología llamada firma digital, basada en la criptografía asimétrica, que, acompañada por determinados procedimientos –como la protección de la clave privada de firma– cumple con todas las características de la firma electrónica avanzada.

3.2.2.1_La identificación del firmante

La firma electrónica avanzada es un mecanismo de identificación superior del firmante, típicamente sustentada en algoritmos de firma digital, una técnica de identificación de entidades de suficiente seguridad y calidad como para recibir efectos jurídicos, cuando cumpla los requisitos que se establecen para ello.

Una firma electrónica avanzada generada por una máquina no va a ser equivalente a una firma manuscrita, aunque identifique a una persona física, a menos que se pueda garantizar que esa persona quería vincularse con la firma, lo cual es un acto humano.

Por ejemplo, una persona que configure su programa de correo electrónico para firmar todos los mensajes puede no estar firmando en el sentido jurídico del término, porque no es consciente de que está firmando: estas firmas electrónicas son avanzadas, pero no son firmas equivalentes a firmas manuscritas.

3.2.2.2_La vinculación única con el firmante

La firma electrónica avanzada tiene una vinculación única con el firmante del mensaje de datos, considerándose firmante a la persona que posee un dispositivo de creación de firma y que actúa en nombre propio o en nombre de una persona física o jurídica a la que representa (artículo 6.2 de la Ley 59/2003).

La vinculación entre firma y firmante –que se denomina autenticación de origen de datos– se logra mediante el empleo de técnicas informáticas basadas en determinados problemas matemáticos: el firmante posee un dispositivo de creación de firma, que contiene unos datos que se emplean para crear la firma.

Tales datos poseen una vinculación matemática con otros datos, que se emplean para verificar la firma electrónica. Los datos de verificación de firma deben ser conocidos por el destinatario del mensaje, que puede emplearlos para comprobar que la firma fue creada por la persona que posee los datos de creación de firma, y no por otra persona.

Precisamente esta característica es la vinculación entre firma y firmante: podemos saber que esa firma corresponde a ese firmante, y no a otro. Esta propiedad viene garantizada, en la firma digital, gracias a la existencia del par de claves –en realidad, gracias a su vinculación matemática- y a la posesión de la clave privada sólo por el firmante.

3.2.2.3_La vinculación con los datos firmados

La firma electrónica avanzada debe permitir la detección de las modificaciones que sufra el mensaje de datos firmado electrónicamente: esta funcionalidad se denomina integridad de los datos firmados.

La firma digital, que se emplea para obtener autenticación (identificación de entidades y de origen de datos), al mismo tiempo garantiza también la integridad de los datos característica de la firma electrónica avanzada.

Ello es consecuencia de una propiedad de las funciones de resumen que se emplean en las firmas digitales, para la comparación del resumen cifrado con la clave privada, que se descifra con la clave pública, con el resumen generado por el destinatario.

Cualquier cambio en el mensaje derivará en la creación por el destinatario de un resumen diferente al resumen que cifró el firmante con su clave privada, de modo que los resúmenes no coincidirán y la firma se verificará incorrectamente: en este caso, la firma ya no está vinculada a los datos firmados, porque el documento no ha permanecido íntegro.

3.2.2.4_El control exclusivo de los medios de creación de firma

La firma electrónica avanzada debe ser «creada por medios que el firmante puede mantener bajo su exclusivo control»(artículo 3.2 de la Ley 59/2003).

Este requisito es una medida de control del uso de la clave privada por parte del firmante, al objeto de sustentar la vinculación real del firmante con la firma.

Si se pudiera demostrar que personas diferentes del firmante tiene acceso a la clave privada, entonces ya no se podría garantizar que las firmas son generadas por el firmante, y por lo tanto, no se podría garantizar la identificación del firmante, ni la vinculación con el firmante, ni la relación existente entre el firmante y el documento supuestamente firmado por él.

3.2.2.5_El reconocimiento jurídico de la firma electrónica avanzada

El reconocimiento jurídico de la firma se establece en dos niveles:

Primero. Todas las firmas electrónicas son jurídicamente aceptables, puesto que no se puede negar efectos jurídicos a la firma electrónica únicamente por el hecho de encontrarse en forma electrónica, o por no basarse en un certificado reconocido, o por no haber sido creada empleando un dispositivo seguro de creación de firma (artículo 3.9 de la Ley 59/2003).

Sin embargo, sí puede negarse efectos jurídicos a las firmas electrónicas que no ofrezcan realmente las garantías de integridad del mensaje, de autenticación de la entidad y de autenticación del origen de los datos.

Por ejemplo: un número de identificación personal (PIN) o una contraseña puede indudablemente servir a los efectos de autenticación de entidades, pero no será considerada una firma electrónica avanzada, porque no garantiza la integridad del documento firmado.

La firma electrónica debe presentar unas características de calidad suficientes, o en otro puede ser considerada inválida por un Juez o un árbitro.

Segundo. Debe existir un contexto legal o contractual que defina los efectos de la firma electrónica, dado que la firma electrónica avanzada no recibe el efecto jurídico típico de la equivalencia con la firma manuscrita directamente de la Ley 59/2003, contexto que recibe un reconocimiento explícito en el artículo 3.10 de la citada Ley, cuando establece que «a los efectos de lo dispuesto en este artículo, cuando una firma electrónica se utilice conforme a las condiciones acordadas por las partes para relacionarse entre sí, se tendrá en cuenta lo estipulado entre ellas.»

3.2.3_*La firma electrónica reconocida*

La firma electrónica reconocida no se definía directamente en el Real Decreto-Ley 14/99, de 17 de septiembre, de firma electrónica, sino que dicha definición se recoge, por fin, en la Ley 59/2003, de 19 de diciembre, de firma electrónica. Se trata de un concepto nuevo demandado por el sector, sin que ello implique modificación alguna de los requisitos sustantivos que tanto la Directiva 1999/93/CE como el propio RDL 14/99 venían exigiendo. Con ello se trata de aclarar que no basta con la firma electrónica avanzada para obtener su equiparación con la firma manuscrita, sino que, de acuerdo con el artículo 3.3 de la Ley 59/2003, se necesitan otros elementos, ya que «se considera firma electrónica reconocida la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma».

Téngase en cuenta que «firma electrónica reconocida» no es toda firma electrónica avanzada, sino sólo un subconjunto de la misma, que está formado por las firmas electrónicas avanzadas de mayor calidad y seguridad, como exponemos más abajo.

La firma electrónica reconocida recibe, respecto del resto de firmas electrónicas, unos efectos concretos directamente de la Ley, que consisten en su equiparación con la firma manuscrita. De esta forma, el artículo 3.4 de la Ley 59/2003 dispone que «la firma electrónica reconocida tendrá respecto de los datos consignados en forma electrónica el mismo valor que la firma manuscrita en relación con los consignados en papel».

Este efecto jurídico es el efecto típico que se entiende para una firma electrónica: la denominación de firma electrónica reconocida se refiere a la cualidad esencial de esta firma, la equiparación directa a la firma manuscrita, allí donde la ley prevea consecuencia en presencia o ausencia de una firma, de modo que no es necesario ni un contrato privado ni una norma jurídica para «reconocer» la firma.

En ausencia de toda otra circunstancia, allí donde la Ley establezca el requisito de la firma o consecuencias en caso de ausencia de una firma, se podrá firmar electrónicamente.

Realmente, la diferenciación entre firma electrónica ordinaria, firma electrónica avanzada y firma electrónica reconocida viene dada por los efectos de la firma frente a terceros, en función exclusivamente de la ca-

lidad de la firma, que deriva de la tecnología y los procedimientos empleados.

La firma electrónica reconocida es un mecanismo de seguridad jurídica, un formalismo que, cuando se cumple, nos protege frente al Estado y a los restantes ciudadanos. Este formalismo emplea unas tecnologías que deben ofrecer unas garantías de calidad y seguridad elevadas, que de algún modo son «reconocidas» por el Estado, sin que sea preciso dictar una nueva norma jurídica para cada posible uso de la firma o llegar a un acuerdo previo con cada persona con la que vayamos a firmar documentos electrónicamente.

Por supuesto, esto no resta valor a los restantes tipos de firmas electrónicas, sean ordinarias, avanzadas o que no cumplan todos los requisitos de la firma electrónica reconocida, tal y como dispone el artículo 3.9 de la Ley 59/2003, al señalar que «no se negarán efectos jurídicos a una firma electrónica que no reúna los requisitos de firma electrónica reconocida en relación a los datos a los que esté asociada por el mero hecho de presentarse en forma electrónica». Sencillamente, el empleo de una firma electrónica reconocida nos garantiza ya el cumplimiento del requisito jurídico de existencia o ausencia de una firma manuscrita.

En los restantes casos, la firma electrónica se podrá emplear en entornos de contratación libre entre las partes o con sustento en normativa administrativa específica, siempre que la legislación aplicable en general permita esta posibilidad (ya que en caso que la exigencia de la firma manuscrita sea imperativa, habrá que valorar la viabilidad de emplear una firma electrónica diferente a la firma electrónica reconocida).

3.2.3.1_La firma electrónica reconocida es una modalidad cualificada de la firma electrónica avanzada

La firma electrónica reconocida es una firma electrónica avanzada (art. 3.2 de la Ley 59/2003), y por tanto, cumple y reúne todas las características de ésta, que hemos visto anteriormente.

No todas las firmas electrónicas avanzadas son susceptibles de ser calificadas firmas electrónicas reconocidas; sin embargo, todas las firmas electrónicas reconocidas son necesariamente firmas electrónicas avanzadas.

3.2.3.2_El certificado reconocido

La firma electrónica reconocida se basa en un certificado digital, que presenta unas elevadas características de calidad y fiabilidad, denominado «certificado reconocido».

Frente al resto de tipos de certificados electrónicos, el certificado reconocido se encuentra cualificado por su relevante uso, conforme al artículo 3.4 de la Ley 59/2003: la equiparación del valor jurídico de una firma electrónica avanzada con el mismo valor jurídico de una firma manuscrita, siempre que dicha firma electrónica avanzada haya sido producida por un dispositivo seguro de creación de firma y esté basada en un certificado reconocido.

Resulta necesario que la firma electrónica que devenga, por efecto de la ley, equiparable a la firma manuscrita, y vaya a ser utilizada en contextos que requieren obtener su misma eficacia jurídica, reúna superiores medidas de seguridad para otorgarle ese reconocimiento legal. La finalidad del certificado reconocido es proporcionar la autenticación de la identidad de una persona con elevados niveles de garantía en el marco de servicios que requieran el (mal) denominado «no repudio»[3]. Por tanto, la firma electrónica que se utilice con este fin debe estar basada en un certificado de elevada calidad, y que se pueda utilizar para confirmar la identidad de la persona que firma electrónicamente, de forma que la identificación de dicha persona resulte altamente fiable.

La fiabilidad del certificado la proporcionan, entre otros: a) los datos de identificación del firmante y otras informaciones que se muestran al usuario en el momento de la verificación del certificado; b) los procedimientos de validación de la información que se hayan utilizado para identificar y comprobar los datos que figurarán definitivamente en el certificado expedido por un prestador de servicios de certificación; y c) las medidas de seguridad adoptadas por el prestador de servicios de certificación en todos los procesos relacionados con la generación, emisión y gestión de los certificados digitales.

Pero además de reunir una elevada calidad, los certificados digitales deben reunir elementos homogéneos para que puedan ser utilizados y

3. En nuestra tradición jurídica, el documento auténtico se corresponde con la garantía que los anglosajones denominan «no repudio».

reconocidos legalmente en todos los Estados miembros, de forma que la heterogeneidad de la normativa en materia de reconocimiento legal de la firma electrónica no entorpezca el uso de las comunicaciones electrónicas y el comercio electrónico.

La fiabilidad de un certificado y de una firma electrónica puede ser definida e interpretada de distintas formas por los distintos Estados miembros. Por ello, se introdujo el concepto de «certificado reconocido» (*qualified certificate*), y la definición de las características que debían reunir este tipo de certificados como soporte de la firma electrónica que obtiene la equiparación con la firma manuscrita. Con la utilización de firmas electrónicas avanzadas basadas en un certificado reconocido, se pretende lograr un mayor nivel de seguridad frente al resto de firmas electrónicas, y que obtengan el reconocimiento en todos los Estados miembros.

El concepto de certificado reconocido viene recogido en el artículo 11.1 de la Ley 59/2003: «Son certificados reconocidos los certificados electrónicos expedidos por un prestador de servicios de certificación que cumpla los requisitos establecidos en la presente Ley en cuanto a la comprobación de la identidad y demás circunstancias de los solicitantes y a la fiabilidad y las garantías de los servicios de certificación que presten». A continuación, el artículo 11.2 de la Ley 59/2003 recoge el contenido mínimo que debe reunir un certificado reconocido, y el artículo 20 de la misma describe las obligaciones exigibles a los prestadores de servicios de certificación que expiden certificados reconocidos.

Resulta de especial relevancia que el prestador de servicios de certificación haya realizado los procedimientos de comprobación de la identidad y demás circunstancias personales de los solicitantes con arreglo a lo dispuesto en el artículo 13 y en el artículo 17 de la Ley 59/2003 (protección de datos de carácter personal), así como garantizar la fiabilidad de los servicios de certificación que prestan, ajustando sus procedimientos a los estándares y prácticas comunes del sector.

3.2.3.3_El dispositivo seguro de creación de firma electrónica

Además de reunir las características de firma electrónica avanzada y estar basada en un certificado reconocido, la firma electrónica reconocida debe ser generada empleando un dispositivo seguro de creación de firma electrónica.

El artículo 24 de la Ley 59/2003, mediante los que se incorpora a la legislación nacional el anexo III de la Directiva, define los datos de creación de firma como «los datos únicos, como códigos o claves criptográficas privadas, que el firmante utiliza para crear la firma electrónica», y a continuación define un dispositivo de creación de firma como «un programa o sistema informático que sirve para aplicar los datos de creación de firma».

De cara a obtener una mayor fiabilidad de la firma generada por los mencionados dispositivos de creación de firma, de forma que sirviera para obtener la denominada firma electrónica reconocida, se determino que los dispositivos de creación de firma que se utilizarán para este propósito debían ofrecer una serie de garantías adicionales, y ser por tanto, más seguros.

De esta forma, un dispositivo seguro de creación de firma se define en la ley como «un dispositivo de creación de firma que ofrece, al menos, las siguientes garantías:

a) Que los datos utilizados para la generación de firma pueden producirse sólo una vez y asegura razonablemente su secreto.

b) Que existe una seguridad razonable de que los datos utilizados para la generación de firma no pueden ser derivados de los de verificación de firma o de la propia firma y de que la firma está protegida contra la falsificación con la tecnología existente en cada momento.

c) Que los datos de creación de firma pueden ser protegidos de forma fiable por el firmante contra su utilización por terceros.

d) Que el dispositivo utilizado no altera los datos o el documento que deba firmarse ni impide que éste se muestre al firmante antes del proceso de firma».

Para proceder a la clarificación de los requisitos enumerados en el Anexo III de la Directiva, e incorporados a nuestra legislación de firma electrónica a través del artículo 24.3 de la Ley 59/2003, de firma electrónica, hay que referirse a las especificaciones técnicas publicadas por el Comité del artículo 9 de la Directiva de Firma Electrónica, o sus equivalentes.

3.2.3.4_El reconocimiento jurídico de la firma electrónica reconocida

El reconocimiento jurídico de la firma electrónica reconocida consiste en el establecimiento del efecto típico de la equiparación con la firma manuscrita:

«La firma electrónica reconocida tendrá respecto de los datos consignados en forma electrónica el mismo valor jurídico que la firma manuscrita en relación con los consignados en papel» (art. 3.4 de la Ley 59/2003)

A la firma electrónica reconocida le otorga la ley directamente la equivalencia funcional con la firma manuscrita respecto de los datos consignados en forma electrónica, sin que sea preciso un acuerdo previo entre las partes ni una norma jurídica administrativa. No basta por tanto con la firma electrónica avanzada para la equiparación con la firma manuscrita; es preciso que la firma electrónica avanzada esté basada en un certificado reconocido y haya sido creada por un dispositivo seguro de creación de firma.

Esta declaración, sin embargo, es tan genérica que en la práctica es preciso establecer contratos referentes al empleo de la firma electrónica en el comercio electrónico –firma electrónica convencional – y dictar normas administrativas para el empleo de la firma electrónica en la Administración electrónica o en documentos privados regulados por la Administración –firma electrónica normativa.

Estos acuerdos y normas establecen con precisión aspectos como el ámbito de utilización, el significado y los concretos efectos de la firma electrónica reconocida.

En relación con el reconocimiento jurídico de la firma electrónica, la Ley 59/2003 de firma electrónica contiene otra novedad respecto a la anterior legislación: la definición de documento electrónico. De acuerdo con el artículo 3.5, «se considera documento electrónico el redactado en soporte electrónico que incorpore datos que estén firmados electrónicamente». El artículo 3.6 establece que «el documento electrónico será soporte de:

a) Documentos públicos, por estar firmados electrónicamente por funcionarios que tengan legalmente atribuida la facultad de dar fe pública, judicial, notarial o administrativa, siempre que actúen en el ámbito de sus competencias con los requisitos exigidos por la ley en cada caso.

b) Documentos expedidos y firmados electrónicamente por funcionarios o empleados públicos en el ejercicio de sus funciones públicas, conforme a su legislación específica.

c) Documentos privados».

Continúa el artículo 3.7 señalando que «los documentos a que se refiere el apartado anterior tendrán el valor y la eficacia jurídica que corresponda a su respectiva naturaleza, de conformidad con la legislación que les resulte aplicable».

En el artículo 3.8 de la Ley 59/2003 se reconoce la admisibilidad como prueba documental en juicio del «soporte en que se hallen los datos firmados electrónicamente». Continua el mencionado artículo estableciendo que «Si se impugnare la autenticidad de la firma electrónica reconocida, con la que se hayan firmado los datos incorporados al documento electrónico, se procederá a comprobar que por el prestador de servicios de certificación, que expide los certificados electrónicos, se cumplen todos los requisitos establecidos en la ley en cuanto a la garantía de los servicios que presta en la comprobación de la eficacia de la firma electrónica, y en especial, las obligaciones de garantizar la confidencialidad del proceso así como la autenticidad, conservación e integridad de la información generada y la identidad de los firmantes. Si se impugna la autenticidad de la firma electrónica avanzada, con la que se hayan firmado los datos incorporados al documento electrónico, se estará a lo establecido en el apartado 2 del artículo 326 de la Ley de Enjuiciamiento Civil».

3.3_Estrategias de empresa en relación con los certificados de identidad y firma electrónica

3.3.1_*Emitir certificados o adquirirlos a un prestador externo*

El primer elemento que hay que determinar en cuanto a la estrategia de los servicios de certificación y de firma electrónica es ciertamente importante, ya que debemos decidir si emitiremos nuestros propios certificados, o si adquiriremos los certificados a un prestador externo, ya que ambas soluciones presentan, por supuesto, ventajas e inconvenientes, y cada organización debe analizar sus propias circunstancias para tomar la decisión más correcta.

Sin ánimo de ser exhaustivos, podemos apuntar algunos criterios:

- La relevancia de la iniciativa en el contexto de la estrategia del negocio. Si para el negocio resulta un elemento absolutamente esencial, bien porque consiste en emitir certificados a cambio de un precio,

bien porque el certificado es el elemento a partir del cual se pueden realizar todos los negocios futuros, entonces puede resultar apropiado expedir. En cambio, si el certificado es un simple accesorio de la actividad, probablemente lo mejor es adquirir.

- El análisis de las necesidades de aplicación, donde resultará esencial el análisis de los requisitos jurídicos de las mismas. Por ejemplo, el tipo de certificado –reconocido, por ejemplo, o en dispositivo seguro– necesario para realizar la transacción.

  Si debemos expedir certificados reconocidos basados en dispositivos seguros, probablemente compensará a partir de un gran volumen de emisión, pero resultará muy caro para pequeñas cantidades.

  En cambio, expedir certificados para usos técnicos, o para usos –también con relevancia jurídica– en grupos controlados o cerrados de usuarios.
- El modelo de inversiones y costes que resulte aplicable en cada caso. Por ejemplo, se puede determinar el coste de las inversiones necesarias para emitir los certificados y compararlo con el coste de adquirir el número de certificados a los diferentes prestadores que operan en el mercado libre, y obtener el punto de equilibrio a partir del cual compensa cada modelo.

  El empleo de servicios de certificación sin coste de licencia, como Microsoft Certificate Services u otros ofrecidos por la comunidad de software libre, como OpenSSL u OpenCA puede modificar las reglas de este punto de equilibrio un poco, pero en todo caso hay que recordar que el mayor coste no viene dado por las licencias, sino por las inversiones en máquinas, los costes de operación y los costes de desarrollo de los aspectos de prácticas del prestador, que aunque se han reducido considerablemente, ciertamente suponen una inversión mínima importante.
- El modelo de retorno de la inversión, que en este caso debe venir dado por los ahorros de coste e incrementos de eficiencia derivados de las diferentes aplicaciones que, sin certificado de firma electrónica, no hubiesen podido ponerse a funcionar.

  En relación con este tercer criterio, hay que decir que aplicar más seguridad de la necesaria suele conducir a una falta de apreciación del valor de la propia seguridad y, en este caso, del valor de usar la firma electrónica. Debemos, en consecuencia, aplicar un modelo propor-

cionado, de acuerdo con el análisis jurídico y con el análisis de riesgo, que también ayudará a recuperar antes las inversiones y a justificar los costes.

En relación con este aspecto de estrategia, hay que decir que el mercado de la firma electrónica en España empieza a estar bastante «maduro», en el sentido de que existe una cierta cantidad y variedad de prestadores de servicios de certificación, públicos y privados, cuyos servicios en algunos casos compiten por la cuota del mercado, mientras que otros servicios resultan complementarios.

Dependiendo de la comunidad de usuarios con la que nos vayamos a relacionar, puede tener sentido o no expedirles certificados, así como dependiendo de la relevancia o visibilidad de los actos jurídicos documentados electrónicamente que vayan a ser autenticados con la firma electrónica de dichas personas.

Por ejemplo, no parece tener mucho sentido para una organización privada expedir certificados a todas las personas con las que tiene relaciones comerciales; en concreto, no parece que el análisis coste-beneficio resulte positivo cuando hablamos de clientes de una o pocas transacciones. Quizá en este escenario sea más lógico el empleo de los certificados que suministran a los ciudadanos la Administración General del Estado o las Administraciones de algunas Comunidades Autónomas, como la Agència Catalana de Certificació con su certificado idCAT.

Por el contrario, puede tener sentido que una organización grande que se relaciona con muchos pequeños proveedores o clientes recurrentes, les suministre certificados para acceder, por ejemplo, a un mercado electrónico controlado por dicha organización, aunque antes de tomar esta decisión, debería analizar el coste-beneficio de adquirir certificados de un prestador privado, como Camerfirma o la Agencia Notarial de Certificación, dado que además de este modo transfiere los riesgos derivados de la provisión de certificados y firmas electrónicas.

En el caso de los profesionales, cuando los mismos se encuentran colegiados, es posible que sencillamente no sea legalmente aceptable que un prestador diferente o no autorizado por el correspondiente colegio profesional expida certificados para dichos profesionales, por lo que habrá que incluir este aspecto en el análisis estratégico.

3.3.2_*Buscar la interoperabilidad y aceptación de los certificados*

El segundo gran aspecto estratégico que debemos considerar es la futura interoperabilidad de nuestros certificados, en especial, cuando los expedimos para su uso por terceros, o bien cuando nos los expedimos a nosotros mismos, para nuestro uso en aplicaciones de terceros.

Una cuestión que podría parece tan evidente se ha convertido, sin embargo, en uno de los más grandes inhibidores del mercado de la certificación, en parte, como dijimos antes, porque una vez que hemos expedido un certificado, no podemos modificarlo, de forma que deberemos revocarlo y expedir otro en su lugar, con el coste extra que ello supone.

Por este motivo, siempre que el certificado deba ser empleado en una aplicación de tercero, debemos asegurarnos legalmente de que podremos hacerlo, mediante la firma del correspondiente contrato, o mediante la superación de los procedimientos administrativos que resulten procedentes, en caso de que el tercero sea una Administración Pública.

Además, deberemos incorporar dentro de los certificados las informaciones –en forma de campos o de extensiones del certificado– que se requieran para garantizar la aceptación de los certificados por los terceros, y la interoperabilidad de los mismos.

Como este objetivo no siempre se puede conseguir, a veces resulta necesario plantearse la expedición de diferentes tipos o clases de certificados, en función de las aplicaciones y de los requisitos de los terceros.

Otra posibilidad radicará en la implantación de tecnologías de validación de firmas electrónicas y de certificados, de forma que sea el tercero destinatario de dichos elementos el que se adapte un poco para entender y poder emplear los certificados, tendencia que cobra fuerza en el mercado de forma progresiva.

3.4_Tipología de certificados de identidad y firma electrónica

En el mercado español existe una variada tipología de certificados de identidad y firma electrónica, adaptados para usos y comunidades de usuarios concretos, que se relacionan a continuación:

- **Certificados ordinarios,** que no cumplen los requisitos legales para la identificación de las personas, que se suelen emplear para el aseguramiento de correo electrónico.
- **Certificados reconocidos,** que cumplen todos los requisitos legales para la identificación de las personas, y que pueden a su vez, clasificarse de la siguiente forma:
  - Certificados de persona física, que actúa como firmante, en nombre propio o en representación de otra persona.
  - Certificados de persona jurídica, a la cual se imputan los documentos firmados, como firmante, en los casos expresamente previstos en la Ley, y sin que sea necesario tener en cuenta los apoderamientos o capacidades de actuación de la persona que custodia el certificado de firma electrónica.
  - Certificados de entidad sin personalidad jurídica, a la cual se imputan los documentos firmados, como firmante, en los casos expresamente previstos en la Ley, y sin que sea necesario tener en cuenta los apoderamientos o capacidades de actuación de la persona que custodia el certificado de firma electrónica.
  - Certificados de representación, en los que deben tomarse en cuenta los apoderamientos y capacidades de actuación de la persona, indicadas o no en el certificado, antes de confiar en la firma. Debe incluir como subtipos los certificados de representación orgánica, voluntaria, etc. Un caso especial es el Certificado de órgano administrativo.
  - Certificados de empleados, en los que además de la identidad personal se indica su vinculación con una organización, sin indicación de apoderamiento.
  - Certificados de profesional colegiado, en los que además de la identidad personal se indica su colegiación en un colegio profesional.
  - Certificados para dispositivos informáticos, incluyendo certificados para servidores seguros, aplicaciones informáticas, firmado de código o estampación de fecha y hora.

4_LA SEGURIDAD Y LA PRESTACIÓN DE SERVICIOS DE LA SOCIEDAD DE LA INFORMACIÓN

4.1_La definición de servicios de la sociedad de la información

Desde una perspectiva práctica, «servicios de la sociedad de la información» es como se ha denominado a aquello que se comercializa a través de Internet, que se consideran servicios que presentan ciertas características particulares, que los diferencian de los servicios de telecomunicaciones/comunicaciones electrónicas y de los servicios audiovisuales.

La definición inicial de servicio de la sociedad de la información se encuentra en la Directiva 98/48, que modifica la Directiva 98/34, que establece un procedimiento de notificación en materia de reglamentaciones técnicas de servicios de la sociedad de la información, definición que ha sido adoptada por la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, en los siguientes términos: «todo servicio prestado normalmente a título oneroso, a distancia, por vía electrónica y a petición individual del destinatario.

El concepto de servicio de la sociedad de la información comprende también los servicios no remunerados por sus destinatarios, en la medida en que constituyan una actividad económica para el prestador de servicios.

Son servicios de la sociedad de la información, entre otros y siempre que representen una actividad económica, los siguientes:

1. La contratación de bienes o servicios por vía electrónica.
2. La organización y gestión de subastas por medios electrónicos o de mercados y centros comerciales virtuales.
3. La gestión de compras en la red por grupos de personas.
4. El envío de comunicaciones comerciales.
5. El suministro de información por vía telemática.
6. El vídeo bajo demanda, como servicio en que el usuario puede seleccionar a través de la red, tanto el programa deseado como el momento de su suministro y recepción, y, en general, la distribución de contenidos previa petición individual.

No tendrán la consideración de servicios de la sociedad de la información los que no reúnan las características señaladas en el primer párrafo de este apartado y, en particular, los siguientes:

1. Los servicios prestados por medio de telefonía vocal, fax o telex.
2. El intercambio de información por medio de correo electrónico u otro medio de comunicación electrónica equivalente para fines ajenos a la actividad económica de quienes lo utilizan.
3. Los servicios de radiodifusión televisiva (incluidos los servicios de cuasivídeo a la carta), contemplados en el artículo 3.a) de la Ley 25/1994, de 12 de julio, por la que se incorpora al ordenamiento jurídico español la Directiva 89/552/CEE, del Consejo, de 3 de octubre, sobre la coordinación de determinadas disposiciones legales, reglamentarias y administrativas de los Estados miembros relativas al ejercicio de actividades de radiodifusión televisiva, o cualquier otra que la sustituya.
4. Los servicios de radiodifusión sonora, y
5. El teletexto televisivo y otros servicios equivalentes como las guías electrónicas de programas ofrecidas a través de las plataformas televisivas.

Resulta positivo que en la definición se incluya una lista de actividades que siempre se consideran servicios de la sociedad de la información, lista que debe entenderse abierta, dado que la definición se refiere a «todo servicio».

4.2_Las obligaciones informativas de los prestadores de servicios

Tanto la Directiva 2000/31 como la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y del comercio electrónico, establecen la necesidad de que los prestadores de servicios se identifiquen electrónicamente y ofrezcan ciertas informaciones mínimas al público en su comunicación telemática, complementando la regulación que ya existía anteriormente.

No hay que pensar que las informaciones que se citan a continuación son las únicas que deben contenerse en las sedes *web* de los prestadores de servicios de la sociedad de la información: por el contrario, se trata de las informaciones que todos los prestadores deben ofrecer; a estas

informaciones hay que añadir las informaciones específicas que la normativa rectora de cada servicio o producto establezca, con independencia del empleo de medios electrónicos para la prestación del servicio o comercialización del producto.

De este modo, el vendedor de información en línea debe ofrece las informaciones que veremos a continuación, pero también las informaciones que se exigen en la Ley de Ordenación del Comercio Minorista para la venta a distancia.

Otro ejemplo sería la agencia de viajes en línea, que debe ofrecer las informaciones contenidas en la Ley 34/2002, de 11 de julio, pero también redactar las ofertas con los contenidos previstos en la Ley de Viajes Combinados.

4.2.1_*La constancia registral del nombre de dominio*

En primer lugar, el artículo 9.1 de la Ley 34/2002, de 11 de julio, establece la obligación de inscribir en el Registro el nombre de dominio empleado por el prestador de servicios de la sociedad de la información, como refuerzo de la tendencia a que la identificación electrónica coincida con la identificación tradicional:

»Los prestadores de servicios de la sociedad de la información establecidos en España deberán comunicar al Registro Mercantil en el que se encuentren inscritos, o a aquel otro registro público en el que lo estuvieran para la adquisición de personalidad jurídica o a los solos efectos de publicidad, al menos, un nombre de dominio o dirección de Internet que, en su caso, utilicen para su identificación en Internet, así como todo acto de sustitución o cancelación de los mismos, salvo que dicha información conste ya en el correspondiente registro».

Esta obligación ha sido muy criticada, por defectos de técnica legislativa en cuanto al procedimiento de «comunicación» a emplear, e indudablemente deberá ser objeto de aclaración posterior, pero no cabe duda de que tiene todo el sentido que el destinatario de servicios de la sociedad de la información pueda obtener la información registral del prestador del servicio a partir del nombre de dominio o la dirección de Internet.

Esta finalidad, sin embargo, se alcanza también mediante la obligación de publicar precisamente la información registral del prestador de servi-

cios de la sociedad de la información, como se establece en el artículo 10.1 de la Ley 34/2002, de modo que puede cuestionarse el acierto de esta prescripción legal, que impone un coste adicional a los prestadores de servicios de la sociedad de la información –el coste de la «comunicación» del nombre de dominio o la dirección de Internet– y no aporta mayor seguridad a los destinatarios de servicios.

Por otra parte, el efecto perseguido puede perderse, desde el momento en que no es obligatoria la «comunicación» de todos los nombres de dominio o direcciones de Internet al Registro: un prestador podría disponer de diversos nombres de dominio, comunicar uno de ellos para cumplir con esta obligación y emplear nombres de dominio no comunicados para actividades cuestionables.

Tras la «comunicación» de los nombres de dominio o las direcciones de Internet, establece el párrafo 2 del artículo 9, que «los nombres de dominio y su sustitución o cancelación se harán constar en cada registro, de conformidad con sus normas reguladoras. Las anotaciones practicadas en los Registros Mercantiles se comunicarán inmediatamente al Registro Mercantil Central para su inclusión entre los datos que son objeto de publicidad informativa por dicho Registro».

La voluntad de coordinar el sistema propuesto con los Registros existentes obliga a realizar una remisión genérica a las normas reguladoras de los mismos, que causa una cierta inseguridad acerca del procedimiento a emplear.

Finalmente, el párrafo 3 del artículo 9 de la Ley 34/2002 establece que «la obligación de comunicación a que se refiere el apartado 1 deberá cumplirse en el plazo de un mes desde la obtención, sustitución o cancelación del correspondiente nombre de dominio o dirección de Internet».

El establecimiento del plazo de un mes hay que ponerlo en relación con la sanción correspondiente para esta infracción, prevista en el artículo 38.4.a), que por ser tener la consideración de sanción leve, trae aparejada multa de hasta 30.000 euros, de acuerdo con lo establecido en el artículo 39.1.c)

Para aquellos prestadores ya establecidos, la disposición transitoria única de la Ley 34/2002, establece el plazo de un año para la «comunicación» del nombre de dominio o de la dirección de Internet:

»Los prestadores de servicios que, a la entrada en vigor de esta Ley, ya vinieran utilizando uno o más nombres de dominio o direcciones de Internet deberán solicitar la anotación de, al menos, uno de ellos en el registro público en que figuraran inscritos a efectos constitutivos o de publicidad, en el plazo de un año desde la referida entrada en vigor».

4.2.2_*La información general a suministrar*

El artículo 10 de la Ley 34/2002 establece la información mínima a suministrar:

»1. Sin perjuicio de los requisitos que en materia de información se establecen en la normativa vigente, el prestador de servicios de la sociedad de la información estará obligado a disponer de los medios que permitan, tanto a los destinatarios del servicio como a los órganos competentes, acceder por medios electrónicos, de forma permanente, fácil, directa y gratuita, a la siguiente información:

   a) Su nombre o denominación social, su residencia o domicilio o, en su defecto, la dirección de uno de sus establecimientos permanentes en España, su dirección de correo electrónico y cualquier otro dato que permita establecer con él una comunicación directa y efectiva.

   b) Los datos de su inscripción en el Registro a que se refiere el artículo 9.

   c) En el caso de que su actividad estuviese sujeta a un régimen de autorización administrativa previa, los datos relativos a dicha autorización y los identificativos del órgano competente encargado de su supervisión

   d) Si ejerce una profesión regulada deberá indicar:

      1r. Los datos del Colegio profesional al que, en su caso, pertenezca y número de colegiado.

      2n. El título académico oficial o profesional con el que cuente.

      3r. El Estado de la Unión Europea o del Espacio Económico Europeo en el que se expidió dicho título y, en su caso, la correspondiente homologación o reconocimiento.

      4t. Las normas profesionales aplicables al ejercicio de su profesión y los medios a través de los cuales se puedan conocer, incluidos los electrónicos.

e) El número de identificación fiscal que le corresponda.

f) Información clara y exacta sobre el precio del producto o servicio, indicando si incluye o no los impuestos aplicables y, en su caso, sobre los gastos de envío.

g) Los códigos de conducta a los que, en su caso, esté adherido y la manera de consultarlos electrónicamente.

2. La obligación de facilitar esta información se dará por cumplida si el prestador la incluye en su página o sitio de Internet en las condiciones señaladas en el apartado 1.»

La primera nota de interés al artículo es su carácter de mínimos, que no excluye la necesidad de cumplir otros requisitos adicionales de información, que pueden venir dados por la aplicación de las normas de comercio minorista –en sede de venta a distancia– o de protección de los consumidores y usuarios. Por ejemplo, la normativa de viajes combinados establece requisitos de información concretos para la oferta al público.

En segundo lugar, hay que señalar que dicha información deberá encontrarse a disposición de los usuarios y de las autoridades de control, en forma electrónica, permanente, fácil, directa y gratuita. Esta obligación del prestador hay que relacionarla con el deber general existente en las relaciones comerciales con consumidores, de redactar las cláusulas de forma comprensible y transparente, evitando oscuridades, criterio que se encuentra recogido en nuestro Código Civil y en la Ley General de Defensa de Consumidores y Usuarios.

Resulta interesante señalar el criterio establecido en el apartado segundo del artículo 10, que facilita la seguridad jurídica en el cumplimiento de la Ley, indicando que el lugar en cierto modo idóneo para la publicación de la información es la página de Internet del prestador.

En la práctica, la forma de cumplir esta obligación es incluir la información en una página, accesible desde la página principal de la sede *web* del prestador, que se suele denominar «Aviso legal». En esta página aparecerá la información exigida por el artículo 10 de la Ley 34/2002, de 11 de julio, y también otras menciones o avisos legales importantes, especialmente referidos a la propiedad intelectual e industrial de los elementos de la página, precauciones que debe tener en cuenta el usuario del servicio y, frecuentemente, la política de protección de datos personales que sigue el prestador de los servicios.

4.2.3_*Información en servicios con uso de «cookies»*

La Ley 34/2002 establece, en su artículo 22.2, en su redacción por Ley 32/2003, las obligaciones en relación con el empleo de «*cookies*»:

»Cuando los prestadores de servicios empleen dispositivos de almacenamiento y recuperación de datos en equipos terminales, informarán a los destinatarios de manera clara y completa sobre su utilización y finalidad, ofreciéndoles la posibilidad de rechazar el tratamiento de los datos mediante un procedimiento sencillo y gratuito.

Lo anterior no impedirá el posible almacenamiento o acceso a datos con el fin de efectuar o facilitar técnicamente la transmisión de una comunicación por una red de comunicaciones electrónicas o, en la medida que resulte estrictamente necesario, para la prestación de un servicio de la sociedad de la información expresamente solicitado por el destinatario.»

Con estas obligaciones se trata de contrarrestar los posibles efectos negativos del empleo de este tipo de dispositivos, tanto desde la perspectiva de la seguridad como desde la perspectiva de la protección de los datos de carácter personal.

4.2.4_*Información en servicios con uso de «dialers»*

Con la aprobación de la Ley 59/2003, de 19 de diciembre, se ha incorporado al artículo 10 de la Ley 34/2002 un nuevo apartado tercero, con el siguiente contenido:

»Cuando se haya atribuido un rango de numeración telefónica a servicios de tarificación adicional en el que se permita el acceso a servicios de la sociedad de la información y se requiera su utilización por parte del prestador de servicios, esta utilización y la descarga de programas informáticos que efectúen funciones de marcación, deberán realizarse con el consentimiento previo, informado y expreso del usuario.

A tal efecto, el prestador del servicio deberá proporcionar al menos la siguiente información:

a) Las características del servicio que se va a proporcionar.

b) Las funciones que efectuarán los programas informáticos que se descarguen, incluyendo el número telefónico que se marcará.

c) El procedimiento para dar fin a la conexión de tarificación adicional, incluyendo una explicación del momento concreto en que se producirá dicho fin, y

d) El procedimiento necesario para restablecer el número de conexión previo a la conexión de tarificación adicional.

La información anterior deberá estar disponible de manera claramente visible e identificable.

Lo dispuesto en este apartado se entiende sin perjuicio de lo establecido en la normativa de telecomunicaciones, en especial, en relación con los requisitos aplicables para el acceso por parte de los usuarios a los rangos de numeración telefónica, en su caso, atribuidos a los servicios de tarificación adicional».

Se trata de una norma específica de información que deberán suministrar los prestadores de servicios de la sociedad de la información que cobren mediante los denominados «*dialers*», que se incorpora debido a los abusos que el empleo de dichas tecnologías ha producido, y que ha supuesto un impacto importante en la seguridad de los usuarios domésticos de servicios telemáticos.

Los «*dialers*» o programas marcadores son aplicaciones informáticas que se descargan desde una página web a la que accede el usuario, y cuya puesta en funcionamiento permite al usuario acceder a visualizar o descargar contenidos y programas de ordenador, mediante la marcación de un número telefónico de tarificación adicional; es decir, un 806, por ejemplo, cuyo coste alcanza los 3 euros por minuto de conexión.

Algunos ejemplos típicos del uso de esta técnica y modelo de negocio son los prestadores de servicios de la sociedad de la información que ofrecen música, videojuegos, horóscopos, contactos, apuestas o sexo y pornografía a través de Internet.

Los programas marcadores vienen firmados electrónicamente por el editor de los mismos, que suele tratarse del mismo prestador de servicios de la sociedad de la información que los emplea para cobrar por la prestación de los servicios, dado que de este modo resulta posible que, con el permiso del usuario, el programa marcador acceda al módem o al enrutador de ADSL al efecto de marcar el número de tarificación adicional.

Sin que quepa objetar nada al modelo de negocio explicado, lo cierto es hasta la fecha su funcionamiento ha dado lugar a no pocos abusos, entre los que podemos citar los siguientes:

a) La falta de información acerca del hecho de que el servicio se presta sujeto a una tarifa adicional. En este caso, el abuso se produce debido al desconocimiento del usuario de que su navegación, aparentemente gratuita, implica una tarifa adicional a través de la factura telefónica.

b) La falta de información absoluta acerca del momento en que se empieza a tarificar extra y en momento en que se vuelve a la tarificación ordinaria. En este caso, el abuso viene determinado por la imposibilidad del usuario de determinar en qué momento empieza a abonar la tarifa adicional.

c) La configuración permanente del número de tarificación adicional como número de acceso a la red Internet. En este caso, el abuso se produce debido a que en la siguiente conexión a Internet –fuera del servicio de pago– el usuario continúa marcando el número de tarificación adicional.

El texto incorporado obliga a los prestadores de servicios de la sociedad de la información a aportar dicha información, con el objeto de reducir los abusos mencionados.

4.3_El tratamiento legal del SPAM o comunicaciones comerciales no solicitadas

La Ley 34/2002, de 11 de julio, regula en su artículo 20 la información exigida sobre las comunicaciones comerciales, ofertas promocionales y concursos. En concreto, la ley establece que las comunicaciones comerciales deben identificarse como tales, y prohíbe su envío por correo electrónico u otras vías de comunicación electrónica equivalente, salvo que el destinatario haya prestado su consentimiento. Asimismo, las comunicaciones comerciales deben indicar la persona física o jurídica en nombre de la cual se realizan.

Asimismo, y en el caso en que tengan lugar a través de correo electrónico u otro medio de comunicación electrónica equivalente (como por ejemplo SMS o MMS), incluirán al comienzo del mensaje la palabra «publicidad».

Por otro lado, en los supuestos de ofertas promocionales, como las que incluyan descuentos, premios y regalos, y de concursos o juegos promocionales, previa la correspondiente autorización, se debe asegurar, además del cumplimiento de los requisitos antes comentados, que queden claramente identificados como tales y que las condiciones de acceso y, en su caso, de participación se expresen de forma clara e inequívoca.

El legislador somete a especial cautela un servicio de la sociedad de la información, consistente en remitir comunicaciones comerciales a usuarios que no las han solicitado específicamente.

A tal aspecto se dedica el artículo 7 de la Directiva:

«1. Además de otros requisitos establecidos en el Derecho comunitario, los Estados miembros que permitan la comunicación comercial no solicitada por correo electrónico garantizarán que dicha comunicación comercial facilitada por un prestador de servicios establecido en su territorio sea identificable de manera clara e inequívoca como tal en el mismo momento de su recepción.

«2. Sin perjuicio de lo dispuesto en la Directiva 97/7/CE y en la Directiva 97/66/CE, los Estados miembros deberán adoptar medidas para garantizar que los prestadores de servicios que realicen comunicaciones comerciales no solicitadas por correo electrónico consulten regularmente las listas de exclusión voluntaria (opt-out) en las que se podrán inscribir las personas físicas que no deseen recibir dichas comunicaciones comerciales, y las respeten.»

Asimismo, la transposición de esta materia en la norma española queda establecida en el artículo 21 de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y del comercio electrónico, al prohibir el envío de comunicaciones publicitarias o promocionales por correo electrónico u otro medio de comunicación electrónica equivalente que previamente no hubieran sido solicitadas o expresamente autorizadas por los destinatarios de las mismas. En este sentido, la prestación de consentimiento expreso exige la manifestación de una voluntad libre, informada, específica e inequívoca de aceptación del envío de comunicaciones comerciales realizadas por correo electrónico u otro medio de comunicación individual equivalente.

Por ello, se entendería cumplido este requisito, por ejemplo, si el prestador de servicios de sociedad de la información, después de informar al

usuario sobre el uso al que destinará su dirección o número de teléfono, le ofrece la oportunidad de manifestar su conformidad con el envío de comunicaciones comerciales haciendo «clic» en una casilla dispuesta al efecto.

Por otro lado, puede entenderse que el requisito no se cumpliría cuando, sin haber autorizado de forma expresa la recepción de comunicaciones comerciales, el destinatario tolera o no se opone a su envío, cuando no responde a los mensajes por los que se solicita su consentimiento[4] y, por supuesto, cuando se hubiera opuesto a su recepción.

El rigor de la norma contenido en el artículo 21 expuesto ha sido suavizado mediante la inclusión de una excepción, en virtud de la disposición final 1.1 de la Ley 32/2003, de 3 de noviembre, de telecomunicaciones, que determina un nuevo apartado 2 del artículo 21 de la Ley 34/2002, de 11 de julio, con la siguiente redacción:

»Lo dispuesto en el apartado anterior no será de aplicación cuando exista una relación contractual previa, siempre que el prestador hubiera obtenido de forma lícita los datos de contacto del destinatario y los empleara para el envío de comunicaciones comerciales referentes a productos o servicios de su propia empresa que sean similares a los que inicialmente fueron objeto de contratación con el cliente.

En todo caso, el prestador deberá ofrecer al destinatario la posibilidad de oponerse al tratamiento de sus datos con fines promocionales mediante un procedimiento sencillo y gratuito, tanto en el momento de recogida de los datos como en cada una de las comunicaciones comerciales que le dirija».

Se trata del caso en que el que un prestador de servicios de la sociedad de la información dispone ya de datos de contacto de correo electrónico de sus clientes, porque ciertamente en este caso obligar a recabar un nuevo permiso del cliente para remitir información adicional sobre productos y/o servicios similares no parecía justificado ni para comerciante ni para cliente.

La referencia a la captación lícita de los datos de contacto resulta algo confusa, dado que la norma parte de la existencia de una relación contractual previa, en la que por supuesto se han obtenido los datos.

4. Se trata, ésta, de una de las prácticas más extendidas en la actualidad.

Probablemente haya que poner este término en relación con la normativa de protección de los datos de carácter personal; es decir, que se debe haber informado al cliente de que sus datos serían tratados para el mantenimiento de la relación comercial.

Más importante resulta el hecho de que la excepción es aplicable para el caso de publicidad sobre productos o servicios similares a los inicialmente adquiridos, y no para los que sean sustancialmente diferentes, lo que limita mucho las posibilidades de uso de esta posibilidad de remitir comunicaciones comerciales no solicitadas.

Lo que probablemente sucederá en este caso es que el prestador aprovechará la oportunidad para solicitar el consentimiento al cliente, para remitirle todo tipo de comunicaciones comerciales.

Se completa el régimen expuesto relativo al SPAM con el establecimiento de los derechos de los destinatarios de servicios expuestos en el artículo 22.1 de la Ley 34/2002, en su redacción dada por la disposición final primera de la Ley 32/2003:

»El destinatario podrá revocar en cualquier momento el consentimiento prestado a la recepción de comunicaciones comerciales con la simple notificación de su voluntad al remitente.

A tal efecto, los prestadores de servicios deberán habilitar procedimientos sencillos y gratuitos para que los destinatarios de servicios puedan revocar el consentimiento que hubieran prestado.

Asimismo, deberán facilitar información accesible por medios electrónicos sobre dichos procedimientos.»

5_LAS OBLIGACIONES DE SEGURIDAD DERIVADAS DE LA PROPIEDAD INTELECTUAL E INDUSTRIAL

Uno de los capítulos importantes - frecuentemente descuidado - a considerar en la estrategia de cumplimiento legal en relación con la seguridad viene referido a las obligaciones de uso de los elementos de propiedad intelectual e industrial de terceros y, en concreto, en relación con el uso de programas informáticos, debiéndose aquí recordar los efectos perversos de las elevadas cotas de piratería informática sobre el mercado.

Desde esta perspectiva, la norma ISO 17799:2005 identifica como control la necesidad de implementar procedimientos adecuados para garantizar el cumplimiento de las restricciones legales al uso del material respecto del cual puedan existir derechos de propiedad intelectual, como derecho de propiedad intelectual, derechos de diseño o marcas registradas.

Los requisitos legales, normativos y contractuales pueden poner restricciones a la copia de material que constituya propiedad de una empresa. En particular, pueden requerir que sólo pueda utilizarse material desarrollado por la organización, o material autorizado o suministrado a la misma por la empresa que lo ha desarrollado.

Los productos de software que constituyan propiedad de una empresa se suministran normalmente bajo un acuerdo de licencia que limita el uso de los productos a máquinas específicas y puede limitar la copia a la creación de copias de resguardo solamente.

La norma recomienda el establecimiento de los siguientes controles jurídicos:

a) publicación de una política de cumplimiento del derecho de propiedad intelectual de software que defina el uso legal de productos de información y de software;

b) la adquisición del software sólo a través fuentes conocidas y serias, para asegurar que los derechos de autor no son violados;

c) mantenimiento de la concienciación respecto de las políticas de adquisición y derecho de propiedad intelectual de software, y notificación de la determinación de tomar acciones disciplinarias contra el personal que incurra en el cumplimiento de las mismas;

d) mantenimiento adecuados de registros de activos;

e) mantenimiento de pruebas y evidencias de propiedad de licencias, discos maestros, manuales, etc.

f) implementación de controles para garantizar que no se exceda el número máximo permitido de usuarios;

g) comprobaciones para verificar que sólo se instalan productos con licencia y software autorizado;

h) emisión de una política para el mantenimiento de condiciones adecuadas con respecto a las licencias;

i) emisión de una política con respecto a la eliminación o transferencia de software a terceros;

j) utilización de herramientas de auditoria adecuadas;

k) cumplimiento de términos y condiciones con respecto a la obtención de software e información en redes públicas;

l) no duplicar, convertir a otro formato o extraer de grabaciones comerciales (película, de audio) otros que permite según la ley de propiedad intelectual;

m) no copiar por completo o en parte, libros, artículos, informes u otros documentos, excepto en los casos que permite la ley de propiedad intelectual.

6_LA CUSTODIA Y ARCHIVO SEGURO DE DOCUMENTOS ELECTRÓNICOS

A medida que se va implantando el documento electrónico original, cobra mayor importancia la estrategia de custodia y archivo seguro de dichos documentos, y de esta forma se refleja en normativa jurídica reciente, como por ejemplo en el caso de la conservación de las facturas electrónicas.

En consecuencia, y desde una óptica general, la norma ISO 17799:2005 considera como control que los registros importantes sean protegidos de pérdidas, destrucción, y falsificación conforme a los requisitos legales, reguladores, convenidos y de negocio.

Los sistemas de almacenamiento de datos deben ser escogidos de tal forma que los datos requeridos puedan ser recuperados en un período y formato aceptable, según las necesidades identificadas.

Los registros deben ser clasificados en diferentes tipos, por ej. registros contables, registros de base de datos, «logs» de transacciones, «logs» de auditoria y procedimientos operativos, cada uno de ellos detallando los períodos de retención y el tipo de medios de almacenamiento, por ej. papel, microfichas, medios magnéticos u ópticos.

Cualquier material criptográfico relacionado y programas asociados con archivos cifrados o firmas digitales, también deben ser almacenados para permitir el desciframiento de los registros durante el tiempo que los

registros son conservados, considerando la posibilidad de degradación de los medios utilizados para el almacenamiento de los registros.

Los sistemas de almacenamiento de datos deben seleccionarse de modo tal que los datos requeridos puedan recuperarse de una manera que resulte aceptable para un tribunal de justicia, por ej. que todos los registros requeridos puedan recuperarse en un plazo y un formato aceptable, y de forma que se puedan cumplir las normas aplicable de archivo histórico, en su caso.

Para cumplir estos objetivos, la norma recomienda el establecimiento de los siguientes controles:

a) Se debe emitir normativa interna para la retención, almacenamiento, manipulación y eliminación de registros e información;

b) Se debe preparar un calendario de retención identificando los tipos esenciales de registros y el período durante el cual deben ser retenidos.

c) Se debe mantener un inventario de fuentes de información clave.

d) Se debe implementar adecuados controles para proteger los registros y la información esenciales contra pérdida, destrucción y falsificación.

7_LA PREVENCIÓN DEL USO INADECUADO DE LOS SISTEMAS DE INFORMACIÓN

Finalmente, resulta de especial importancia establecer las bases jurídicas para la regulación del uso de los sistemas de información por parte de los usuarios, especialmente en el caso del uso no autorizado o del abuso de los sistemas.

A esta problemática dedica un control específico la norma ISO 17799:2005.

La dirección debe aprobar el empleo de instalaciones procesamiento de información. Cualquier empleo de estas instalaciones para propósitos no comerciales sin la aprobación de la dirección, o para cualquier propósito no autorizado, deberían ser considerados como un empleo inadecuado de las instalaciones.

Esta norma implica la necesidad de supervisar el empleo de los sistemas de información, actividad siempre conflictiva, dado que el derecho legal

de control del trabajo por las organizaciones nunca puede conculcar derechos fundamentales, como el que asiste a los trabajadores en el empleo razonable de medios empresariales para la actividad privada. Caso paradigmático de este conflicto es la monitorización del correo electrónico, que puede ser tipificada como un delito caso que se realice sin las debidas garantías legales.

En cualquier caso, y con independencia del necesario y delicado análisis jurídico previo al establecimiento de medidas técnicas para el control de las actividades de las personas que trabajan o colaboran con una organización, si se identifica cualquier actividad no autorizada, esta actividad debe ser atendida por la dirección, y se deben aplicar las medidas disciplinarias apropiadas y, en su caso, las acciones legales oportunas.

Como contrapartida del derecho de supervisión de la organización, todos los usuarios deben ser conscientes de su acceso permitido y de las medidas de supervisión implantadas con el objetivo de detectar el empleo no autorizado de sistemas de información.

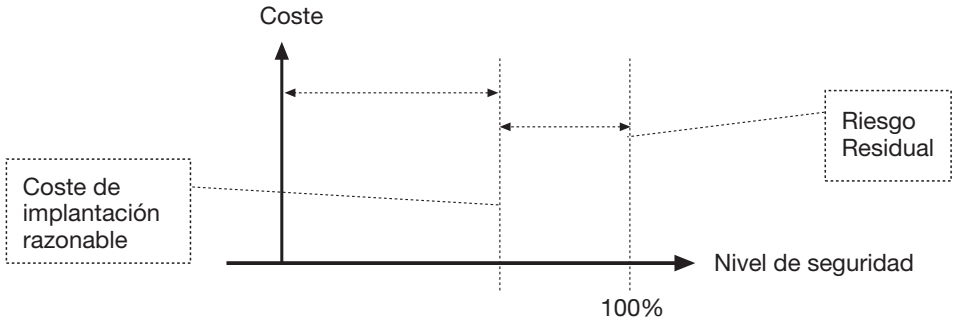
Típicamente, esto puede ser logrado concediendo a los usuarios la autorización por escrito, mediante una copia que debería ser firmada por el usuario y conservada por la organización. Los empleados de una organización, contratistas, y usuarios terceros deben ser informados de sus accesos autorizados.

Las herramientas de seguridad y sus costes

Ramiro Muñoz
Director técnico de Camerfima, CISA

En este capitulo nos centraremos en describir las herramientas que podemos utilizar para proteger nuestros activos en el mundo electrónico. Ofreceremos cuando así sea posible una valoración de sus costes. Hay que destacar que los costes son puramente referenciales obtenidos en algunos caso de los proveedores o de catálogos públicos. En algunos casos por la sensibilidad de la información no hemos podido obtener precios concretos de los productos.

Es ya sabido (por la reiteración del concepto) que la seguridad total no existe y si existiera seria carisima, habría que añadir. Algo menos sabido es que a partir de un punto cuanto más se invierte en medidas de seguridad, menos incremento supone en la misma. Veamos lo anteriormente dicho en un gráfico:



Es muy difícil llegar a la seguridad 100% ya que los costes se disparan exponencialmente, por lo tanto es recomendable quedarse en una inversión razonable que cubra la mayor parte de nuestros riesgos. Debemos elegir soluciones adecuadas y proporcionadas ya que no deberíamos dedicar más recursos económicos a proteger un activo del valor del propio activo.

El primer paso por consiguiente es realizar lo más detalladamente posible un análisis de riesgos. Este análisis nos ayudara a localizar nuestros riesgos y asegurarnos medidas proporcionadas.

En pocas palabras un análisis de riesgos consiste en:

- **Inventariar los activos** que queremos proteger y valorarlos. Esta valoración no es solo económica sino que se tendrán en cuenta otros valores intangibles como la imagen de la empresa. Normalmente necesitamos proteger los datos de la empresa relativos al personal, funciones, almacén, pedidos, albaranes, ordenes de compra...etc. Esta valoración para simplificar puede ser un tanto subjetiva indicándolo una escala del 1 a 5.
- **Localizar sus vulnerabilidades**. Un ordenador necesita electricidad para funcionar, por lo tanto deberemos asegurar el suministro eléctrico para que los datos contenidos en el ordenador sean accesibles.

  Es recomendable y gratuito incorporarse a una lista de distribución de noticias de seguridad como hispasec http://www.hispasec.com. Hispasec tiene un servicio sobre seguridad que nos mantienen al día, mediante el envío de correos electrónicos, sobre posibles vulnerabilidades en productos informáticos.
- **Detectar las amenazas**. Si no existen amenazas seria necesario proteger un activo. En nuestro caso deberíamos detectar las posibles amenazas que puedan actuar sobre alguno de nuestros activos. En nuestro ejemplo, una caída de electricidad.

  No debemos olvidar en ningún momento aquellas que afectan al cumplimiento de normativas jurídicas. Entre estos deberíamos tener en consideración:

  – La protección de datos personales.

  – La protección de los registros de la organización

  – Derechos de propiedad intelectual.
- **Valorar el impacto**. Tendremos que valorar el impacto de que una amenaza aproveche una vulnerabilidad de nuestro activo y produzca un daño. La valoración también es algo subjetivo y podemos ayudarnos de nuevo de una ponderación entre 1 y 5.
- Una vez que tenemos valorados todos estos parámetros estamos en disposición de **calcular el riesgo** de cada amenaza. El riesgo es la

probabilidad de que se materialice una amenaza. Nos toca ahora a nosotros decidir que nivel de riesgo queremos asumir.

Nos podemos ayudar de esta tabla para decidir donde debemos tomar medidas y donde el riesgo no es suficiente para la implantación de un control:

Probabilidad	1					2					3					4					5				
Impacto	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4
Valor																								
1	3	4	5	6	7	4	5	6	7	8	5	6	7	8	9	6	7	8	9	10	7	8	9	10
2	4	5	6	7	8	5	6	7	8	9	6	7	8	9	10	7	8	9	10	11	8	9	10	11
3	5	6	7	8	9	6	7	8	9	10	7	8	9	10	11	8	9	10	11	12	9	10	11	12
4	6	7	8	9	10	7	8	9	10	11	8	9	10	11	12	9	10	11	12	13	10	11	12	13
5	7	8	9	10	11	8	9	10	11	12	9	10	11	12	13	10	11	12	13	14	11	12	13	14

de 3 a 7	No es necesario control
de 8 a 10	Control recomendado
de 11 a 15	Control obligatorio

- Una vez conocida el riesgo asociado a las amenazas que pueden causarnos daños en nuestros sistemas deberemos ponernos manos a la obra implantado controles para:

  Eliminarlo o Atenuarlo o Asumirlo o Diferirlo.

Para eliminar o atenuar el riesgo contamos con herramientas o controles que nos permiten realizar dicha acción.

La necesidad primordial de invertir en controles de seguridad es evitar otros costes, los costes que suponen los posibles incidentes de seguridad. Existen costes directos como la perdida de ingresos ocasionada por una parada de los sistemas informáticos debido a una incidencia de seguridad, a los que habría que añadir el coste de devolver el sistema al estado en que estaba antes del incidente. Entre los costes indirectos estaría la pérdida de imagen o la pérdida de confianza de nuestros clientes, estos valores son mas difíciles de cuantificar numéricamente pero es necesario hacerlo aunque sea de una manera subjetiva. Se puede aplicar entonces una sencilla regla matemática donde la inversión en controles de seguridad menos los costes de las perdidas estimadas por incidencias de seguridad debe ser obligatoriamente mayor que cero.

La inversión en sistemas de seguridad no es en muchos casos entendida suficientemente por los altos responsables de la empresa ya que se asignan directamente como gastos. Esta decisión no se debe tomar desde la perspectiva de un escenario sin incidencias sino desde la previsión o la recreación de escenarios donde se han materializado posibles ame-

nazas de seguridad. Por otro lado y siguiendo con reglas obvias pero no siempre aplicadas, la inversión en seguridad debe ser suficiente para permitir cumplir los objetivos de negocio.

Desde el punto de vista del retorno de la inversión en seguridad los controles de seguridad se dividen en aquellos que reducen la vulnerabilidad y aquellos que reducen el impacto, estas últimas se pueden asociar a medidas preventivas. Las que reducen el impacto pueden describirse como medidas correctivas, es decir medidas que se toman una vez producido el incidente.

Se debe por lo tanto (siempre de una manera subjetiva, ya que difícilmente tendremos inicialmente datos concretos de incidencias posibles) calcular el coste de la inversión para implantar las medidas preventivas y correctivas. Este dato será una marca estimativa que nos indicara si la inversión en controles de seguridad es adecuada o no. Periódicamente y en base a la experiencia acumulada las previsiones de costes se irán ajustando a valores más reales.

1_HERRAMIENTAS PARA EL CONTROL DE LA SEGURIDAD

Como medida de orden vamos a clasificar los controles de seguridad tomando como base los capítulos del estándar ISO 17799 que establece un código de buenas prácticas para la gestión de sistemas informáticos.

Como base para el desarrollo de este apartado del libro determinamos pasar rápidamente por aquellos capítulos del estándar que no tengan que ver con su objetivo concreto, es decir la descripción de las herramientas de seguridad y sus costes. Muchos de los controles sugeridos en el estándar tienen que ver con la redacción y aplicación de políticas y procedimientos que no afectan a herramientas concretas de seguridad. No obstante es fundamental que el uso las herramientas de seguridad sean fruto de una planificación ordenada en base a la aplicación de políticas y procedimientos de seguridad.

Los apartados de la ISO7799 son:

1. **Política de seguridad**: documento de política de seguridad y su gestión.
2. **Control de accesos**: requisitos de negocio para el control de accesos; gestión de acceso de usuario; responsabilidades del usuario; control de

acceso en red; control de acceso al sistema operativo; control de acceso a las aplicaciones e informaciones; informática y conexión móvil.

3. **Gestión de las comunicaciones y las operaciones**: Procedimientos y responsabilidades de operación; gestión de servicios de terceras partes; planificación y aceptación del sistema; protección contra software malicioso; backup; gestión de seguridad de redes; utilización de soportes de información; intercambio de información y software; servicios de comercio electrónico; monitorización
4. **Adquisición, desarrollo y mantenimiento de sistemas de información**: requisitos de seguridad de los sistemas de información; procesamiento correcto en aplicaciones; controles criptográficos; seguridad de los ficheros del sistema; seguridad en los procesos de desarrollo y soporte; gestión de vulnerabilidades técnicas. Gestión de incidentes de seguridad: comunicación de eventos y puntos débiles de seguridad de la información; gestión de incidentes y mejoras de seguridad de la información.
5. **Seguridad física y del entorno**: áreas seguras; seguridad de los equipos.
6. **Conformidad**: con los requisitos legales; políticas de seguridad y estándares de conformidad y conformidad técnica; consideraciones sobre la auditoría de sistemas de información.
7. **Seguridad ligada a los recursos humanos**: anterior al empleo; durante el empleo; finalización o cambio de empleo.
8. **Aspectos organizativos para la seguridad**: organización interna; organización externa.
9. **Gestión de activos**: responsabilidad sobre los activos; clasificación de la información.
10. **Gestión de continuidad del negocio**: aspectos de la seguridad de la información en la gestión de continuidad del negocio.

1.1_Política de seguridad

El objetivo de este capitulo del estándar es proveer guía y asesoramiento en la seguridad de la información para que se alinee perfectamente con los requerimientos de negocio y la regulación jurídica aplicable.

La política de seguridad debe ser el documento guía para la gestión de los recursos informáticos.

1.2_Control e acceso lógico

Objetivo del control es organizar el acceso lógico a la Información, es decir los controles que necesitaremos implantar para proteger los datos desde los aplicativos, los sistemas operativos o las conexiones remotas.

Vamos entonces a aplicarnos en el control de acceso a la información en los equipos informáticos que la custodian. La primera barrera al acceso lógico del ordenador debe ser la contraseña BIOS (Sistema Básico de Entrada/Salida), esta solución evita el acceso a atacantes poco especializados y además es gratuita.

Otra regla de uso común y recomendable es la configuración de protectores o bloqueadores de pantalla que evitan el acceso a nuestro puesto de trabajo cuando tenemos que ausentarnos. En los sistemas Windows por ejemplo se accede mediante las teclas Alt-Ctr-Del.

Contraseñas o (Passwords)

El acceso por contraseña es el sistema de autenticación mas usado y extendido, es un mecanismo que ha perdurado desde los orígenes de la informática en sistemas multiusuario. El mecanismo consiste en pedir un nombre de usuario o identificativo y para este nombre una contraseña que debe coincidir con aquella guardada por el equipo al que se accede, para ese usuario en particular.

El acceso por usuario y contraseña es un método barato y sencillo que ha permanecido mucho tiempo en vigor y que se resiste a desaparecer. Es evidente que por el contrario las amenazas han evolucionado notablemente en el mundo informático. El sistema de contraseña es fácilmente atacable, sobretodo si no se siguen algunas recomendaciones:

- Evitar las claves genéricas de acceso.
- Bloqueos de contraseñas después de varios intentos fallidos.
- Cambios periódicos de la contraseña.
- Las claves de acceso deben cumplir una política rigurosa respecto a su composición (dígitos, signos y números) de tal forma que no sean fácilmente atacables. Por otro lado las contraseñas deben ser a la vez fácilmente recordables a fin de evitar tener que escribirlas en un papel.

La autenticación por contraseña es lo que se llama un sistema de factor simple (accedemos por algo que sabemos). Existen sistemas mas fiables llamados de factor doble (algo que sabemos y algo que tenemos) incluso sistemas de factor triple (algo que sabemos algo que tenemos y algo que somos).

Por una razón u otra nos vemos por lo tanto a día de hoy en la necesidad de gestionar múltiples contraseñas, y si no queremos utilizar siempre la misma (algo radicalmente desaconsejable) deberemos ayudarnos de herramientas de gestión de contraseñas como **PasswordSafe** o **Keepass** de distribución gratuita y que permite la gestión de múltiples contraseñas recordando solo una.

[Single Sign-on (La contraseña única)

¿Como podríamos resolver el problema de la múltiple identificación?. Una primera aproximación puede ser la asignación al usuario del mismo nombre en todos los sistemas y por supuesto las contraseñas. Es difícil mantener la misma contraseña en todos los sistemas, diferentes sistemas tienen diferentes reglas para las longitudes y formatos de las contraseñas y diferentes periodos de validez. Incluso aunque se consiguiera mantener la misma contraseña para todos los sistemas o recordar la especifica de cada uno, el usuario tiene que realizar log-in (identificación y autenticación) en cada sistema cada vez que se accede.

Todo esto produce en las organizaciones una pérdida de productividad notable y el incremento en los riesgos de seguridad. El uso de usuario y contraseña por lo tanto es uno de los sistemas de autenticación existentes más populares pero al mismo tiempo más débiles que seguramente se irán sustituyendo por sistemas mas adecuados.

Los sistemas de Sigle Sign-on (Una sola contraseña para todos los servicios) permiten, una vez autenticados en un sistema, poder «navegar» por otros sin tener que identificarnos nuevamente.

Podemos realizarlo mediante programas que «capturan» peticiones de usuario y contraseña, estos programas identifican a la máquina y cuando esta nos piden identificarnos el programa actúa ofreciendo los datos que previamente nosotros hemos introducido en una pequeña base de datos.

Podemos usar directorios estándar tipo LDAP para identificar de forma centralizada a los usuarios. Las aplicaciones que entiendan este protocolo utilizarán una base de datos común para identificar al usuario.

Otra modalidad de identificación única (y la mas pura) es pasar las acreditaciones de la persona identificada de un sistema a otro.

Productos de Sigle Sign-ON y accesos lógicos.

- **Passlogix** (comercial)
- **pGina** (acceso a los sistemas utilizando diversos mecanismos de autenticación) distribución gratuita.
- **Kerberos** sistema de tikets. distribución gratuita.
- **AC Camerfirma. DFirma Gina** Las credenciales de acceso al sistema son almacenadas de forma segura, mediante su cifrado con el certificado digital almacenado en el chip. Realiza la autenticación de red sobre Active Directory de Windows.
- **AC Camerfirma. DFirma Web Secure** Sistema que permitirá la integración, de la autentificación con certificados digitales en las aplicaciones Web con garantías de desconexión por inactividad.
- **AC Camerfirma DFirma Web Sign On**. Solución para almacenar las credenciales de acceso a cualquier entorno Web de terceros (Web del banco, WebMail,…) en tarjetas criptográficas. Las credenciales son almacenadas de forma segura, mediante su cifrado con el certificado digital almacenado en el chip. Una vez almacenadas en la tarjeta, el sistema al detectar el acceso a dichas páginas Web, introducirá automáticamente las credenciales de acceso una vez el usuario haya introducido el PIN de la tarjeta. De esta forma el usuario sólo necesitará recordar el PIN de acceso a su tarjeta criptográfica.

Federación de identidades

La federación de identidades es el planteamiento de la contraseña única o Sigle Sign On llevada a un nivel mas amplio sobrepasando los ámbitos de una empresa, es decir, propone que un usuario pueda autenticarse una vez y saltar de servicio en servicio Web sin tener que identificarse nuevamente. Los sistemas trasladan bajo la autorización del usuario la información sobre su identidad. El referente en este tipo de servicios es

Liberty Alliance que se encarga de acreditar productos que cumplen los requerimientos del sistema para integrarse en un sistema de identificación única.

Una herramienta a tener en cuenta en el ámbito de identidad federada es Cardspace la solución de Microsoft. Cardspace es un gestor de identidades que permite al usuario gestionar diferentes identidades, ya sean elaboradas por el mismo o por terceras partes.

Cuando accedemos a un servicio electrónico que necesita identificarnos Cardspace le presenta al usuario una cartera con diferentes tarjetas de identidad (diferentes datos y acreditaciones) el usuario elige con que tarjeta quiere identificarse de tal forma que no ofrecerá mas información al sistema de la que realmente necesita para obtener el servicio.

Sistemas Biométricos

Los sistemas biométricos emplean rasgos de la persona como las huellas digitales, iris o voz (algo que somos) para la autenticación en servicios electrónicos. Los sistemas más usados actualmente son los de huella digital. Permiten acceso a equipos informáticos e incluso se integran con otros sistemas de autenticación para dotarle de un factor adicional, por ejemplo para el acceso a tarjetas criptográficas.

Contraseñas de un solo uso (OTP: One Time Password)

Sistemas de OTP (One Time Password) Contraseñas de un solo uso (algo que tenemos y algo que sabemos).

El sistema de contraseñas de un solo uso permite utilizar un dispositivo (hardware o software) para calcular en un momento concreto una clave de acceso. Con esta clave y un PIN personal podremos acceder al servicio durante un periodo muy corto de tiempo. El sistema de autenticación del equipo conectado sincroniza también el valor de la clave en función del usuario y la hora de producirse la acreditación.

Certificados Digitales

Sistema de identificación de doble factor algo que tenemos (clave criptográfica privada) y algo que sabemos (PIN de activación de la clave). Ver apartado dedicado a los certificados digitales.

Gestión de Privilegios

Hay que diferenciar los sistemas de autenticación lógica (sabemos quien es) de los sistemas de permisos o privilegios (que puede hacer). La gestión de ACL (Access Control List) Listas de control de acceso permiten controlar los permisos sobre los recursos gestionados.

El uso de directorios centralizados tipo LDAP como Active Directory de Microsoft permiten realizar una política de permisos de acceso a los recursos gestionados mediante ACL (Listas de control de Accesos). Estas listas permiten asignar recurso de acceso, lectura, escritura borrado de recursos en base a una identificación previa.

1.3_Control de las comunicaciones y de las operaciones

Objeto: Garantizar operaciones correctas y seguras en el proceso de información. Los procesos operativos deberán especificar instrucciones detalladas para realizar cualquier operación.

Protección contra código malicioso. Proteger la integridad del software y de la información.

Prácticamente todo el mundo es consciente de las amenazas que supone un acceso a Internet, ningún usuario a día de hoy accede a Internet sin tener al menos un antivirus instalado en su equipo. Sin embargo el problema más común es que una vez instalado la sensación de seguridad crece de forma desproporcionada e injustificada. Un antivirus no es la solución, por ejemplo si este no se actualiza de forma periódica. Para ello es necesario que nuestro proveedor disponga de un servicio de actualización en línea y que configuremos nuestro antivirus para que cada vez que nos conectemos a Internet busque nuevas actualizaciones.

Los virus se aprovechan de vulnerabilidades del sistema operativo o de las aplicaciones, por lo tanto es fundamental para la seguridad de los recursos informáticos tener instaladas las últimas versiones y parches de los sistemas y aplicaciones.

Los programas antivirus actuales suelen incorporar ya herramientas antispyware spam y otros mecanismos de protección contra ataques habituales:

- **Spyware.** Programas que roban información del usuario y la trasmiten a terceros.
- **SPAM.** Correo electrónico no deseado «correo basura»
- **Firewall. Firewall personal**. Gestión de políticas de acceso (entrada/salida) a las aplicaciones del equipo. Mediante unas reglas de actuación decimos al ordenador que peticiones de entrada salida están permitidas.
- **Anti-Dialers.** Control del marcado automático a sitios externos, este ataque es efectivo si tenemos configurado el sistema para acceder a Internet vía línea telefónica común y MODEM.
- **Fishing**. Robo de contraseñas mediante links en el correo electrónico que nos trasladan a sitios Web fraudulentos pero con un aspecto igual al original. Normalmente en servicios bancarios.

Herramientas:

- **Marca comercial: AVG**
  AVG Anti-Virus Free Edition. Edicion Gratuita para usos no comerciales.
  Contiene: Antivirus, Anti-Spyware, Firewall personal, Anti SPAM
- **Marca comercial: Avast**
  Avast Home Edition. Edición Gratuita para usos no comerciales.
  Avast Profesional Edición
- **Marca comercial: Panda**
  Panda Internet Security 2007
  spyware, hackers, estafas online

Otros

NOD32, kaspersky

Soluciones especificas Spyware freeware:

- **Ad-Aware**
- **Spybot.**

Todo lo anterior es útil en un escenario de un único puesto de trabajo conectado a Internet. Cuando tenemos que proteger equipos desde los cuales ofrecemos servicios electrónicos o tenemos una red corporativa a proteger, el problema debemos de abordarlo de diferente manera. Dependiendo de la criticidad deberíamos valorar la incorporación de un antivirus perimetral. Un antivirus perimetral controla el tráfico de una sec-

ción de red y es capaz de detectar un ataque antes de que llegue al destino final. Obviamente esto no exime de tener protegido el equipo de usuario, que debe tener su propia protección individual complementándose con la ofrecida por el antivirus perimetral. Recordar que es altamente recomendable que los productos utilizados en el antivirus perimetral y el local deben ser de diferentes proveedores, esto nos protege de posibles errores en alguno de los suministradores.

Podemos encontrar dispositivos que ya incorporan diferentes controles de seguridad perimetral.

- **E-Safe:** Aplicativo de gestión de antivirus perimetral. Controla el trafico WEB, el de correo (SMTP) el trafico de trasmisión de ficheros (FTP).
- **Panda:** Panda Gate Defender solución perimetral de Firewall, IPS, VPN, Anti-malware, Content Filter, Anti-spam y Filtrado web.

Firewall (cortafuegos) (control preventivo).

El cortafuegos es un elemento de seguridad perimetral que permite aplicar políticas de permisos sobre el trafico recibido desde una red de comunicaciones.

La ubicación habitual de un cortafuegos es el punto de conexión de la red interna de la organización con la red exterior (Internet), de este modo se protege la red interna de intentos de acceso no autorizados desde dichas redes, que puedan aprovechar vulnerabilidades de los sistemas de la red interna.

También es frecuente conectar a los cortafuegos una tercera red, llamada zona desmilitarizada o DMZ, en la que se ubican los servidores de la organización que deben permanecer accesibles desde la red exterior. Servicios WEB por ejemplo.

Los servidores en Internet utilizan direcciones de red IP para ser accedidos que pueden ser invocadas desde los clásicos nombres de dominio de todos conocidos como www.miempresa.com. Dentro de un mismo servidor existen puertos de escucha para ofrecer diferentes servicios. Por ejemplo el puerto 80 escucha peticiones de los navegadores para servirles páginas. El puerto 443 escucha peticiones de paginas seguras HTTP...etc. Por lo general cuando instalamos una maquina nueva por defecto muchos de estos puertos están abiertos de serie y es recomen-

dable cerrarlos. Un cortafuegos permite que aunque tengamos estos puertos abiertos se apliquen políticas que no permitirían su acceso si no esta expresamente autorizado por el administrador. **La política inicial de un cortafuegos es: Todo esta prohibido menos lo que expresamente este permitido. A partir de aquí se van incorporando reglas de permisos y puertos de acceso.**

Actualmente los antivirus comerciales y el propio sistema operativo incorporan cortafuegos personales integrados que es necesario configurar y que aportan seguridad adicional a los dispositivos cortafuegos perimetrales.

Existen soluciones de cortafuegos en software que podemos instalar en una maquina sobre Linux y que permitirían obtener una solución de cortafuegos con costes reducidos aunque se necesitan conocimientos avanzados para si instalación y mantenimiento.

Herramientas:

- **Fortinet: FortiGate.**Solución perimetral de Firewall, antivirus, IDS Intrusiones, VPN.

  FortiGate-50A está dirigido a aplicaciones de necesidad de pequeñas oficinas y oficinas en casa. Proporciona una completa protección en tiempo real a través de combinaciones de antivirus basados en red (antivirus perimetral), filtrado de contenido Web y de correo electrónico, firewall (perimetral) , VPN, detección y prevención de intrusos basados en red (IDS perimetral) y desvío de red. Diseñado para trabajadores de casa y pequeñas oficinas remotas con 5 o menos empleados.

  El rango de precios varían en función del numero de usuarios remotos. rendimiento. Los costes pueden aumentar hasta los 8.000 para 1.500 usuarios.

  Fuente Fujitsu España.

Otros:

- **Checkpoint,** Firewall VPN soluciones de alta disponibilidad.
- **Nokia** IP560

IDS (control preventivo)

La detección de intrusiones es el proceso de monitorizar los eventos que ocurren en un sistema o red, para analizarlos en busca de problemas de seguridad en base a patrones predefinidos que ofrecen indicios de que el sistema puede estar siendo objeto de un ataque.

SNORT. Herramienta de prevención de intrusiones de código abierto y libre distribución capaz de realizar un análisis del trafico de la red en tiempo real, analiza el trafico de paquetes IP para detectar patrones de posibles ataques.

Integridad (preventiva)

Los sistemas informáticos deben garantizar su integridad de forma que podamos detectar cualquier manipulación no autorizada . Una modificación no controlada de un sistema operativo puede suponer dos cosas: o bien que algún usuario o administrador de éste ha realizado cambios no controlados o documentados, o bien que se ha producido una intrusión en el mismo. Un sistema de verificación de integridad nos permitirá descubrir de forma rápida si alguna parte del sistema se ha visto modificada desde la última vez que realizamos el control.

Dentro de las herramientas utilizadas para este fin, la más conocida sin duda es Tripwire, un desarrollo del proyecto COSAT de la Universidad de Purdue. Esta herramienta está disponible bajo licencia libre, aunque la empresa Tripwire ofrece versiones propietarias con funcionalidades adicionales y también ofrece herramientas de control de integridad para entornos más especializados (dispositivos de red). Además de Tripwire, existen otras alternativas con licencia de software libre como Integrit, Samhain, Osiris, Syscheck, Aide y Fcheck entre otras.

Los propios sistemas operativos de los ordenadores incorporan herramientas de integridad en su configuración de serie:

Sistema operativo	Herramientas integradas en el sistema operativo
Debian GNU/Linux Mandrake Linux SuSE Linux Xarxa Hat Linux	Sistema de gestión de paquetes (dpkg ó rpm) La mayoría de las de libre distribución
FreeBSD NetBSD OpenBSD	La mayoría de las de libre distribución (en la colección de ports)
HP-UX	Product Description File cksum
Solaris	ASET (Automated Security Enhancement Tools)
Windows (Me, XP)	Windows System Restore

Políticas de eliminación de software ilegal. (Control preventivo)

Es evidente que una de las amenazas posibles a considerar seriamente es la violación de la propiedad intelectual. Cada producto de terceros que utilicemos debe estar respaldado por su licencia correspondiente. Para estos menesteres una herramienta de referencia puede ser TS Census. TS Census proporciona una serie de herramienta que nos permite realizar:

- Inventario de activos informáticos software y hardware.
- Control del cumplimiento de licencias.
- Control de uso de los aplicativos.

Backups. (Control correctivo)

Una de las herramientas correctivas más eficaces para recuperar el estado de un sistema a la situación anterior a una incidencia es la realización de copias de backup. Siendo un aspecto tan importante no existe una concienciación adecuada incluso dentro de los profesionales informáticos. En la mayoría de los casos los backups no se gestionan de forma correcta, incluso en algunos casos directamente no se realizan. Nada hay más frustrante que perder en trabajo de varios días por la falta de un sistema de backup adecuado.

Hoy en día existen multitud de herramientas que permiten la automatización de las copias de backup pudiéndose realizar de manera transparente para el usuario y minimizando las perdidas de información.

SYNCBACK. Es una herramienta como otras muchas que permite la realización centralizada de backups. SYNCBACK permite la recolección de información de los puestos de usuario a un sistema centralizado donde se van incorporando los nuevos ficheros encontrados o las actualizaciones. La recuperación de los datos se puede realizar mediante el acceso al sistema central.

La recogida de información se puede programar de tal forma que esta se realice en momentos de menos carga de trabajo.

Tendremos que evaluar la «ventana de riesgo» entre copias de backup. Si realizamos una copia diaria, en el caso peor podríamos perder información de un día completo de trabajo.

Existen servicios de backup remotos que recogen los datos de los equipos de usuario y lo almacenan en ubicaciones externas. Este servicio por

supuesto simplifica y abarata los costes de implantación pero incorpora un riesgo adicional al enviar nuestros datos a empresas externas. En estos casos deberemos asegurarnos de que los datos solo salen cifrados y permanecen cifrados en los equipos del proveedor.

Un ejemplo de servicio de este tipo ofrecido por Arsys.

512 MB	14,90 €/mes
1 GB	29,00 €/mes
2 GB	59,00 €/mes
5 GB	119,00 €/mes

Datos de Arsys Online Backup

Backup incremental

Una forma de utilizar de forma mas eficiente los sistemas de backup es ir haciendo solo copia de aquella información añadida o modificada sobre los datos ya guardados, en vez de ir creando copias completas. Es lo que llamamos backups incrementales.

Los backups incrementales necesitan de una gestión ordenada, disponiendo de copias completas duplicadas y las diferentes copias de los backups incrementales hasta llegar a una recuperación completa del sistema.

Copias en caliente

En algunos casos debido a la criticidad de los datos deberíamos tener copias de estos en caliente es decir copias replicadas en el mismo momento de producirse algún cambio en los datos. Para protegerlos de amenazas físicas la copia en caliente puede estar ubicada en un lugar remoto, en algunos casos pueden existir requerimientos de distancias mínimas entre los dos puntos (incluso en placas tectónicas diferentes).

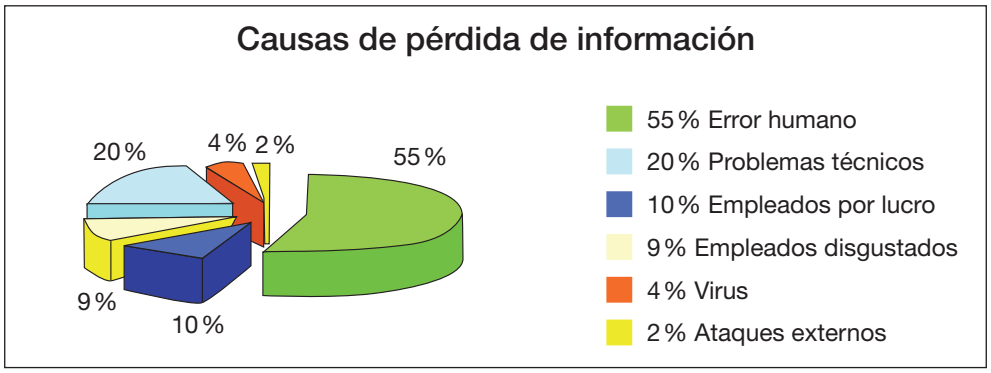
Cifrado de backups

Los dispositivos de almacenamiento que contienen información de copias de seguridad deben estar protegidos convenientemente. Es aconsejable tener una caja de seguridad ignifuga para su almacenamiento en las instalaciones de la empresa y en instalaciones de seguridad externas. La caja de seguridad de un banco puede ser una solución aceptable y económica.

- **Viceversa** es una herramienta de copia y sincronización de fichero de bajo precio que puede sernos útil a la hora de replicar nuestros ficheros y mantenerlos cifrados para su posterior envío o custodia. http://www.tgrmn.com/

Custodia de Datos Electrónicos

Existen servicios profesionales de custodia de información como Iron Mountain o European Security. Estos servicios recogen los dispositivos en la propia empresa y los trasladan con seguridad a sus dependencias donde son custodiados de forma segura.



Fuente: *Computer Security Institute.*

Los datos de backup que revelan las actividades de los sistemas (registros) o información sensible de negocio deben estar cifrados para evitar el acceso de terceros no autorizados.

Recuperación de sistemas

En algunos casos necesitamos no solo recuperar los datos de un sistema informático, sino el sistema completo, es decir bases de datos, sistemas operativos, configuraciones, aplicativos....etc. que hemos perdido por ejemplo por que hemos tenido un error irrecuperable en un disco. Necesitamos entonces reproducir desde cero todo el sistema.

Tenemos soluciones interesantes para la recuperación de sistemas como:

- Acronis trueimage para la recuperación de sistemas en entorno Windows y Linux
- Symantec backup EXEC

Gestión de la seguridad en las redes

En redes abiertas como Internet la seguridad de la información en transito es un requisito básico. La tecnología sobre la que se basa Internet no se pensó para dotarla de seguridad, sino más bien de robustez y disponibilidad.

Disponemos de varios mecanismos para asegurar las comunicaciones.

Protocolo SSL, TSL (Para entornos WEB)

SSL/TSL proporciona autenticación y privacidad de la información entre extremos sobre Internet mediante el uso de criptografía. Normalmente accedemos a este protocolo cuando tecleamos en un navegador https:// en vez del clásico http://.

El proceso se realiza mediante la presentación desde el servidor de páginas Web de un certificado digital que acredita la dirección Web que hemos escrito en el navegador y su propietario. También establece un canal seguro cifrando la información enviada entre cliente y servidor.

La versión 3 del protocolo SSL, permite la identificación por el mismo medio del cliente que accede a la Web. En este caso al cliente le será exigido un certificado digital válido como elemento de autenticación. En este escenario obtenemos a) una identificación del servidor, b) identificación del cliente y c) un canal cifrado. Como vemos unas garantías suficientes para ofrecer servicios vía Web seguros.

El establecimiento de estos protocolos no incorporan más gastos adicionales que la configuración del servidor de páginas Web y la adquisición de los certificados de servidor seguro y cliente.

VPN

La mayoría de los productos de cortafuegos (Firewall) permiten la configuración de canales de conexión segura vía VPN (Virtual Private Network), Red Privada Virtual.

Se trata de fabricar un canal seguro extremo a extremo, de la misma forma que lo hace el protocolo SSL en entornos WEB. Las conexiones VPN Permiten conectar de forma segura distintas oficinas utilizando redes pu-

blicas como Internet. La sensación es la de tener una propia red privada como indica su nombre. La utilización de Internet reduce considerablemente los costes de comunicación en las empresas en detrimento tecnologías antiguas como las líneas punto a punto.

La configuración de una red VPN permite en muchos casos el desarrollo del telé-trabajo al ofrecer un canal seguro de acceso a los servidores centrales de la compañía desde el hogar del tele-trabajador.

También podemos conectar equipos de comunicación de dos sedes de una empresa con los propios enrutadores de las oficinas a través del establecimiento de una VPN encargándose estos dispositivos de hacer que las redes de las dos sedes sean virtualmente la misma.

Existen soluciones especializadas en dispositivos hardware que ofrecen un rendimiento mejor. Podemos encontrar productos de proveedores como Nortel, Cisco, Linksys, Netscreen, Symantec, Nokia, US Robotics, D-link etc. Existen tambien soluciones software con un rendimiento menor pero mucho mas baratos ya que se configurarían en el propio sistema operativo Linux o Windows. Existen implementaciones de codigo abierto como **OpenSSH**, **OpenVPN** y **FreeS/Wan**.

Certificados digitales

El certificado digital es un elemento de control de riesgo electrónico en el proceso de identificación. La utilización de usuario y contraseña comúnmente utilizadas demuestran una fortaleza limitada al asegurar la identidad del usuario electrónico, sobre todo cuando se utilizan contraseñas débiles formados por números o palabras del diccionario fácilmente atacables.

El certificado digital es un elemento de autenticación de doble factor, es decir «algo que se sabe» PIN de activación de la clave y «algo que se tiene» la clave.

El certificado digital se basa en tecnología criptográfica de clave pública. La tecnología de clave pública consiste en la generación de dos claves criptográficas complementarias. Una clave es llamada «pública» ya que se dará a conocer a todos y otra «privada» que es custodiada y conocida solo por el usuario. Cuando se cifra un mensaje con una clave la otra clave complementaria puede descifrarlo y viceversa.

La custodia de la clave privada puede hacerse mediante un fichero software protegida por una contraseña o en una tarjeta criptográfica con una contraseña de acceso.

El mecanismo técnico del funcionamiento de la tecnología de clave pública es el siguiente: cuando «A» usa la clave privada para cifrar un mensaje este puede ser recuperado por «B» usando la clave publica de «A» de tal forma que si esto se produce podemos asegurar que el mensaje ha sido originado por «A», el poseedor de la clave privada.

Este hecho produce la autenticación del usuario «A» sin tener que enviar ningún dato privado por la red.

También podemos usar la tecnología de clave pública para cifrar el contenido de un documento o mensaje. Si «B» cifra un mensaje con la clave publica de «A» se asegurará que solo «A» con su clave privada puede acceder al contenido del documento.

El certificado digital es simplemente un documento electrónico emitido por una tercera parte de confianza (Prestador de Servicios de Certificación, PSC) acreditando que la clave pública matemáticamente relacionada con la clave privada esta asociada a una identidad concreta.

Es importante valorar al emisor del certificado (PSC) para que el sistema de autenticación y cifrado tenga el soporte suficiente. Un mismo PSC puede emitir diferentes tipos de certificados para diferentes usos y ofreciendo garantías diferentes.

Analizaremos en la siguiente tabla los prestadores de certificación españoles y los tipos de certificados que emiten

Nombre comercial	Entidad emisora	Uso	Colectivo	Observaciones/ Precio de referencia
DNI-electrónico	Direcció General de la Policia	Autenticación	Ciudadano	
DNI-electrónico	Direcció General de la Policia	Firma electrónica	Ciudadano	
Certificado Empresarial de Pertenencia	AC Camerfirma	Firma electrónica Cifrado Autenticación	Empleados de entidades jurídicas en general. Autónomos	30 € + IVA 2 años Software 65 € + IVA 2 años tarjeta o token
Certificado Empresarial de Representación	AC Camerfirma	Firma electrónica Cifrado Autenticación	Representantes de entidades jurídicas en general. Autónomos	60 € + IVA 2 años Software 95 € + IVA 2 años tarjeta o token
Certificado de Persona Jurídica	AC Camerfirma	Firma electrónica Cifrado Autenticación	Entidades jurídicas en general. Autónomos según normativa AEAT	60 € + IVA 2 años Software 95 € + IVA 2 años tarjeta o token
Certificado de Factura Electrónica	AC Camerfirma	Firma electrónica de facturas	Empleados de entidades jurídicas en general. Autónomos	400 € + IVA 2 años Software 435 € + IVA 2 años tarjeta o token
Certificado de Servidor Seguro	AC Camerfirma	Autenticación de servidor de páginas HTTPS	Direcciones Internet (URL)	210 € + IVA 3 años
Certificado de Sello de Empresa	AC Camerfirma	Firma electrónica	Entidades jurídicas en general. Autónomos	Firma avanzada 500 € + IVA 3 años
Certificado de Firma de Codigo	AC Camerfirma	Firma de desarrollos, Applets, Activex, exe, dll, etc.	Entidades jurídicas en general. Autónomos	650 € + IVA 3 años
Certificados Notariales Personales	ANCERT	Firma digital Autenticación Cifrado	Personas físicas	120 € + IVA 3 años tarjeta
Certificados Notariales Corporativos	ANCERT	Firma digital Autenticación Cifrado	Personas jurídicas	140 € + IVA 3 años tarjeta
Certificados Notariales Corporativos de Representación	ANCERT	Firma digital Autenticación Cifrado	Representantes de personas jurídicas. Apoderados generales. Apoderados mercantiles	140 € + IVA 3 años tarjeta
Certificados Notariales Personales de Representación Personal	ANCERT	Firma digital Autenticación Cifrado	Representantes de personas físicas. Apoderados generales. Apoderados mercantiles	140 € + IVA 3 años tarjeta

Nombre comercial	Entidad emisora	Uso	Colectivo	Observaciones/ Precio de referencia
Certificados Notariales de Servidor Seguro	ANCERT	Autenticación de servidor de páginas HTTPS	Direcciones Internet (URL)	500 € + IVA 3 años
Certificados Corporativos Reconocidos	AC Abogacía. Autoridad de Certificación de la Abogacía	Firma digital Autenticación Cifrado	Colegiados	Solo colegiados 3 años
Certificados de Clase 2 de Personas Físicas	ANF Asociación Nacional de Fabricantes	Firma digital Autenticación	Personas físicas	Tarjeta 70 € + IVA 2 años
Certificados de Clase 2 de Personas Físicas	ANF Asociación Nacional de Fabricantes	Firma digital Autenticación	Personas jurídicas	Tarjeta 120 € + IVA 2 años
Certificados para Colegios Profesionales	Firma profesional	Firma digital Autenticación Cifrado	Colegiados	Precio según volumen de certificados y servicios contratados
Certificados para Persona Vinculada	Firma profesional	Firma digital Autenticación Cifrado	Empleados	120 € + IVA 3 años soporte tarjeta o token a parte
Certificados para Facturación Electrónica	Firma profesional	Firma digital	Emisión de factura electrónica	350 € + IVA 2 años, soporte tarjeta o token a parte
Certificados para Persona Jurídica	Firma profesional	Firma digital Autenticación Cifrado	Entidades jurídicas	120 € + IVA 2 años, soporte tarjeta o token a parte. Condiciones especiales para fundaciones
Certificados de Servidor Seguro	Firma profesional	Autenticación de servidor de páginas HTTPS	Direcciones Internet (URL)	200 € + IVA 2 años. Consultar otros períodos y certificados multidominio
Certificado Personal de Identificación y Firma Reconocida y Certificdo Personal de Cifrado (CPISRC-1 + CPX-1):	CATCERT	Firma digital-autenticación y cifrado en dos certificados separados	Personal de la administración pública catalana	Soporte tarjeta, 4 años 28 €
Certificado Personal de Identificación y Firma Reconocida con Cargo y Certificado Personal de Cifrado con Cargo (CPISRC-1 + CPXC-1):	CATCERT	Firma digital-autenticación y cifrado en dos certificados separados	Personal de la administración pública catalana con cargo	Soporte tarjeta, 4 años 28 €
Certificado de Entidad de Firma Reconocida y de Entidad de Cifrado (CESR-1 + CEX-1):	CATCERT	Firma digital-autenticación y cifrado	Entidades jurídicas	Soporte tarjeta, 4 años 28 €
Certificado de Dispositivo Servidor (CDS):	CATCERT	Autenticación de servidor de páginas HTTPS	Direcciones Internet (URL)	Soporte software 4 años 300 €
Certificdo de Dispositivo de Programa (CDP)	CATCERT	Firma de desarrollos, Applets, Activex, exe, dll, etc.	Administraciones públicas catalanas	Soporte tarjeta 4 años 500 €

Nombre comercial	Entidad emisora	Uso	Colectivo	Observaciones/ Precio de referencia
Certificado de Dispositivo de Aplicación (CDA)	CATCERT	Firma electrónica	Administraciones públicas	Sofware 4 años 300 €
Certificado de Persona Física	CERES (FNMT)	Firma digital Autenticación Cifrado	Personas físicas	En software y tarjeta
Certificado de Persona Jurídica	CERES (FNMT)	Firma digital Autenticación. Cifrado	Personas jurídicas	En software y tarjeta
Certificados Reconocidos en SW y HW	Autoridad de Certificación de la Generalitat Valenciana (ACCV)	Firma digital-autenticación y cifrado en dos certificados separados	Ciudadanos Comunidad Valenciana	44,57 € los de tarjeta. Gratuitos los de software. 3 años
Certificados Reconocidos de Entidad	Autoridad de Certificación de la Generalitat Valenciana (ACCV)	Firma digital Autenticación Cifrado	Empresas de la Comunidad Valenciana	44,57 € en tarjeta 3 años
Certificado de Entidad de las Administraciones Públicas	IZEMPE	Firma digital-autenticación y cifrado en dos certificados separados	Personas que ejercen cargos en entidades públicas	En tarjeta
Certificado de Ciudadano	IZEMPE	Firma digital-autenticación y cifrado	Ciutadà	En tarjeta
Certificado de Entidad	IZEMPE	Firma digital Autenticación, Cifrado	Persona jurídica	En tarjeta y Software
Certificado de Pertenencia a Entidad	IZEMPE	Firma digital Autenticación, Cifrado	Persona física de pertenencia a empresa	
Certificado de órgano Administrativo	IZEMPE	Firma digital Autenticación, Cifrado	Órgano administrativo	Software
Certificado Corporativo Reconocido	IZEMPE	Firma digitall-autenticación y cifrado en dos certificados separados	Personas que desempeñan cargos administrativos sin potestades administrativas	En tarjeta
Certificado Corporativo No Reconocido	IZEMPE	Firma digital-autenticación y cifrado en dos certificados separados	Personas que desempeñan cargos administrativos sin potestades administrativas	En tarjeta y Software
Certificado de Dispositivo Informático (1)	IZEMPE	Autenticación de servidor de páginas HTTPS	Direcciones Internet (URL)	
Certificado de Dispositivo Informático (2)	IZEMPE	Firma digital-	Máquina	
Certificado de Firma de Código	IZEMPE	Firma de desarrollos Applets, Activex, exe, dll, etc.	Desarrollos	
Certificados Reconocidos BANESTO	BANESTO	Firma digital Autenticación Cifrado	Clientes y accionistas de BANESTO	
Certificados de Clase 2	TELEFÓNICA	Firma digital Autenticación Cifrado	Personas físicas	
Certificados Reconocidos de Clase 3	Colegio de Ingenieros de Caminos CICCP	Firma digital Autenticación, Cifrado	Colegiados	En tarjeta

Otros servicios de los prestadores de Certificación

Validación de los certificados

Un aspecto a importante a considerar en el uso de los certificados digitales es el proceso de validación de estos. Un certificado digital tiene una duración temporal (como vemos en la tabla anterior). Dentro de este periodo de validez el certificado puede perder su efectividad por diferentes causas (robo, perdida del PIN de activación, cambio de datos...etc.) en este caso el certificado debe ser revocado y el prestador debe hacerlo publico. Una persona o una aplicación deben verificar un certificado digital antes de darlo como válido.

La forma que un prestador tiene para hacer público este hecho es mediante:

- **CRL:** Listas de revocación (Certification Revocation List). Son listas negras de certificados que estando en vigor han perdido su efectividad.
- **OCSP:** (Online Certificate Status Protocol) Servicio de consulta del estado de los certificados. La consulta se realiza accediendo a un servicio online y recibiendo una respuesta inmediata sobre el estado del certificado en cada momento.

Un certificado digital debe ser verificado en el momento de su uso efectivo (al autenticarse, al producir una firma o al cifrar datos). Es entonces cuando debemos estar seguros de su validez. Por este hecho que se aconseja siempre que sea posible incorporar el estado del certificado en origen.

Algunos prestadores de certificación ofrecen el acceso al sistema de validación con una contraprestación económica, deberemos por lo tanto tener en cuenta este aspecto. Actualmente solo los certificados CERES (FNMT) tienen esta carga. Los demás prestadores tienen al menos disponibles de forma gratuita el acceso a las CRL.

Sellos de tiempo

Otro servicio ofrecido por los prestadores de servicios de certificación es el sellado de tiempo. El sellado de tiempo consiste en asociar un documento o transacción a una fecha y hora concreta recogida de una fuente fiable y firmado electrónicamente por el Prestador del servicio. Un sello de tiempo es una evidencia electrónica de que un documento o transacción existía en una fecha concreta.

Este servicio complementa el uso de los certificados digitales para asegurar por un tercero (y no por la fecha recogida en el ordenador del usuario) la fecha y hora en la cual se ha producido su uso y por tanto la aplicación correcta del estado del certificado (revocado o activo).

Algunos prestadores como obligan a la obtención del sello de tiempo cada vez que se utilizan sus certificados, de esta forma incorporan la validación en origen siempre que se utilizan.

Para ser correcta una firma electrónica debería incorporar:

1. La firma, los certificados implicados,
2. El estado de estos mediante CRL/OCSP
3. El sello de tiempo.

Los sellos de tiempo se distribuyen generalmente por suscripciones o compra de lotes de sellos.

El certificado Digital y su aplicación en la gestión de la seguridad de Sistemas de Información

El certificado digital como elemento de control de riesgo es muy efectivo en diferentes aspectos de la gestión de la seguridad en los sistemas de Información.

- Autenticación:

Para acceso físico a los equipos (móviles o de sobremesa). Para ello contamos con sistemas de Smatcardlogon que se pueden configurar en redes corporativas, siempre que el certificado este incorporado en una tarjeta o en un dispositivo USB.

En la misma tarjeta que da soporte al certificado se puede incorporar tecnología RFID (identificación vía radio) para el acceso físico a áreas restringidas.

La misma tarjeta donde es ubica el certificado puede servirnos de identificación física al poder incorporar nuestra foto y datos personales impresos.

La misma tarjeta puede utilizar una banda magnética para el control de acceso a las instalaciones o el control de entradas/salidas del personal.

El certificado puede identificar y cifrar canales de comunicación empleando protocolos SSL. Este protocolo es el usado en muchos servicios de páginas Web mediante accesos HTTPS. El certificado de Servidor asegura la identidad del sitio Web y el cifrado del canal de datos. Este mecanismo es importante cuando recogemos datos personales por ejemplo en formularios Web.

El certificado puede no solo identificar al sitio Web sino que también puede hacerlo con usuario que accede. Mediante la configuración de nuestro servidor de páginas WEB podemos pedir una identificación mediante certificado digital a nuestro visitante en áreas restringidas de nuestro servicio. De esta forma en un sitio Web podríamos tener la identificación del servidor la identificación del usuario y el canal de datos cifrado.

El certificado también puede servir para firmar electrónicamente programas que se ejecutan en los navegadores como activex, applets java...etc. de esta forma conoceremos: quien lo ha desarrollado, y si ha sido modificado el código antes de ejecutarlo. También puede firmar macros de Office con el mismo objetivo.

- Firma electrónica:

El certificado digital es actualmente la referencia principal de la firma electrónica , en este caso deberemos distinguir varios aspectos y tipos de firma ya que en este caso existen implicaciones jurídicas a la hora de utilizar uno u otro tipo.

- **Firma electrónica avanzada:** Ofrece garantías técnicas de origen e integridad de los documentos o transacciones electrónicas firmadas aunque no tiene valor jurídico directo sino que debe argumentarse la prueba en caso de un proceso legal.
- **Firma electrónica reconocida o cualificada:** Ofrece garantías de origen e integridad de los documentos o transacciones electrónicas firmadas. Tiene valor jurídico equivalente a la firma manuscrita.

Podemos emplear la firma electrónica para garantizar la integridad de ficheros, documentos y transacciones.

- Cifrado:

Otro aspecto importante que nos ofrecen los certificados digitales es la posibilidad de cifrar información. El cifrado de información es un proceso

delicado y con alto riesgo ya que si no somos cuidadosos podemos perder fácilmente la información cifrada. Como hemos visto utilizamos la clave pública asociada al certificado para cifrarlos, luego necesitaremos la clave privada para recuperarlos y por lo tanto es fundamental tener acceso a esta en todo momento, para lo cual realizaremos copias de seguridad. Es altamente recomendable usar un certificado expresamente emitido este uso.

Windows ofrece la posibilidad de configurar el sistema EFS de cifrado de archivos y discos duros mediante certificados emitidos por terceras partes.

- *Wireless.* **Tecnología Inalámbrica**

Las redes inalámbricas cada vez están copando una mayor cuota de mercado, evitar tener que realizan complejas instalaciones de cableado y garantizar la movilidad de los dispositivos es un aliciente importante. El uso de esta tecnología tiene sus desventajas:

- Todos los que estén en un radio de 100 ms. aprox son intrusos potenciales.
- La información se transmite por el aire y, por lo tanto, puede ser «vista» por cualquiera que esté en el radio de 100 ms.
- Nuestros usuarios pueden conectarse equivocadamente (o voluntariamente) a redes que se encuentren abiertas en el radio de 100 ms y esto puede ser muy peligroso para la seguridad de nuestra organización
- Cualquier «vecino» puede captar los login y las contraseñas cuando los usuarios intentan conectarse

Por lo tanto deberemos configurar los mecanismos de seguridad para evitar los problemas asociados a esta tecnología.

Activar siempre la conexión cifrada mediante cifrado **WAP** con clave de al menos **128** bits

Existen soluciones en el mercado de puntos de acceso WIFI que incorporan cortafuegos y protección contra intrusión y antivirus como **FortiWiFi-60.**

- Externalización (Outsourcing):

Una alternativa a tener en cuenta en la gestión de seguridad de sistemas informáticos es trasferirla a un tercero, es decir, realizar un outsourcing o externalización. Esta alternativa no implica la perdida de responsabilidad

ya que jurídicamente siempre recae en el propietario del servicio. Va a depender de como tramitemos los servicios de externalización, de que estas responsabilidades puedan ser traspasadas a la empresa proveedora de los servicios o no. La externalización ofrece riesgos significativos sobre todo si no hay una trascripción clara de los servicios ofrecidos y sus niveles de calidad acordados.

La gestión de la seguridad de los sistemas informáticos no es el objetivo fundamental de negocio en la mayoría de las empresas, el objetivo es vender sus productos y/o servicios, por lo tanto parece razonable dejar la gestión de los sistemas informáticos en manos de los expertos. Existen como en todas las cosas puntos a favor y en contra a la hora de elegir la externalización.

La cesión de los mecanismos de seguridad a un tercero por lo anteriormente dicho exige una cierta madurez en el conocimiento de los mecanismos de seguridad (o una fe ciega en el proveedor de servicios). Por lo tanto no debería tomarse esta decisión como una solución para evitarse complicadas lucubraciones técnicas o el establecimiento de políticas de seguridad ya que estas decisiones deben ser en ultimo caso asumidas por el cliente.

Negociar un acuerdo de externalización suele ser un proceso complejo: adaptación de los procesos de negocio, cesión o adquisición de hardware y software, el establecimiento de indicadores para comprobar el cumplimiento de los niveles de servicio esperados y el cumplimiento de las políticas de seguridad de la organización. Estos elementos deben quedar claramente referidos en los acuerdos del nivel del servicio (SLA Service Level Agreement) y ser monitoreados de manera regular a fin de prevenir su incumplimiento. Un SLA por lo tanto debe describir con exactitud los servicios ofrecidos, las herramientas de control del nivel del servicio y la penalización en caso de incumplimiento.

Conceptos del contrato de servicios externalizados:

- HOSTING

  Alberque de los servicios en maquinas propiedad del proveedor.

  – Compartido (con otros servicios)

  – Dedicado (maquina de uso exclusivo)
- HOUSING

  – Albergue de un equipo del cliente en instalaciones del proveedor

- COMUNICACIONES
  - – Configuración del ancho de banda necesario para ofrecer el servicio.
- SEGURIDAD PERIMETRAL (FIREWALL / IDS)
  - – Cortafuegos, IDS, Antivirus
- BACKUP
  - – Operaciones de los Backups en los equipos albergados.
- SEGURIDAD FISICA
  - – Características del la sala de operadores donde esta alojado
- MONITORIZACION
  - – Servicios de control del rendimiento de la plataforma y detección de incidentes
- ALERTAS
  - – Avisos sobre incidencias ocurridas.
- INFORMES
  - – Informes periódicos de los servicios ofrecidos

Ejemplo estimativo de costes mensuales de un servicio de externalización en modalidad de housing.

- **Alojamiento** servidor 2U (tamaño del equipo enracable), incluye conexión a red, **Monitorización Básica** 24*7 Direccionamiento IP 55,00 €
- **BACKUP** Centralizado 1 Servidor (1 agente S.O.) hasta 20 GB (1,75 € por GB adicional) 85,00 €
  Caudal **Conectividad** Internet (1 Mbps) 275,00 €
- **Seguridad Perimetral** 2 puertos 79,00 €

Herramientas para la Facturación Electrónica

He querido incorporar en este apartado soluciones para la realización de facturación electrónica. La realización de facturación electrónica permitirá un ahorro importante de costes en la gestión de este tipo de operaciones, permitiendo sustituir los procesos manuales actuales por la tramitación electronica.

Convertir un documento físico en uno electrónico es relativamente fácil bastaría con utilizar un escáner, o mas fácil aun elaborar directamente una factura en formato electrónico. La transformación de este documento en una factura electrónica jurídicamente válida requiere de la firma electrónica que le dota de autenticidad e integridad. La AEAT ha elaborado una lista de emisores acreditados para la emisión de certificados que pueden ser usados para la elaboración de factura electrónica que publica en su página web.

Las herramientas por lo tanto para realizar facturación electrónica serian las mismas que para la elaboración de una firma:

- Office XP puede incorporar firma en documentos word o excell
- Firma de un correo electrónico Outlook, Thunderbird de Mozilla, etc.
- Herramientas de firma desktop como Dfirma Desktop de AC Camerfirma (Gratuito)
- Firma de PDF Acrobat Writer (300)..etc

Pero existen soluciones más especializadas para la gestión de la factura electrónica que nos permiten una integración con los sistemas existentes de elaboración de factura y contabilidad. Es aconsejable que plantearse la implantación de facturación electrónica como un proceso completo.

Las **Cámaras de Comercio** va a abordar de manera inminente un proyecto de plataforma de facturación electrónica que permitirá la gestión de factura electrónica de forma fácil para la empresas.

EDICOM también posee una plataforma para la gestión externalizada de factura electrónica.

IPSCA tiene soluciones de automatización de factura electrónica.

AC Camerfirma también ofrece soluciones de firma de factura en su producto Dfirma Batch Server.

Aspectos a considerar:

- Formato de la factura (La AEAT esta promocionando un formato de factura que exigirá a sus proveedores y que por lo tanto tendrá un efecto mimético importante en la industria. Se puede descargar de su página Web. www.aeat.es

- Acceso a la validación de los certificados asociados a la firma. El proveedor seleccionado debe ser sensible a la necesidad de acceder sin coste a las listas de revocación.
- Existe la posibilidad de almacenar las facturas en papel en formatos electrónicos siempre que se realice la transformación (de formato físico a electrónico) con un sistema homologado por la AEAT.

1.4_Adquisición de equipamiento

Asegurar que la seguridad es una parte integral de los sistemas de información.

Los sistemas de información incluyen sistemas operativos, infraestructuras, aplicaciones de negocio, productos comerciales, servicios y las aplicaciones desarrolladas ad hoc. El diseño y la implementación de un sistema de información que soporta procesos de negocio es de vital importancia para garantizar su seguridad. Los requerimientos de seguridad deben ser identificados antes de su desarrollo.

Gestión de claves criptográficas

Todas las claves criptográficas deberán ser protegidas contra modificación, pérdida o destrucción. Adicionalmente las claves deberán protegerse contra usos no autorizados. Los equipos usados para generar almacenar claves criptográficas deberán estar físicamente protegidos.

La gestión de claves puede realizarse en contenedores software o hardware. Lo mas habitual y aconsejable es mantener claves en soportes criptográficos (hardware) especialmente diseñados para ello.

Tarjetas criptográficas: Estos dispositivos tienen un sistema operativo que previene os ataques sistemáticos contra el PIN de acceso, bloqueando el dispositivo después de varios intentos. Almacenamos claves simétricas, certificados e incluso almacenes de contraseñas.

Ejemplos de Proveedores: Bit4id, GyD, Aladdin, Microelectronica

Como vemos, podemos encontrar estos dispositivos también en formato token USB y variaciones y complementos como funcionalidades de contacless (inalámbricas) para identificación de presencia sin contacto en las tarjetas o dispositivos de contraseña única (OTP).

Para almacenar claves en servidores, por ejemplo en plataformas de firma o cifrado de documentos, emisión de factura electrónica o establecimiento de canales cifrados SSL o VPN tenemos otros tipo de dispositivos como los HSM (Módulos de seguridad Hardware) y aceleradores criptográficos. Estos dispositivos están especializados en la generación de claves criptográficas y su mantenimiento seguro, a parte de funcionar como una ayuda complementaria para descargar al sistema soporte de las pesadas tareas criptográficas.

Algunos proveedores:

Microelectronica, Eracom (Safenet), nCipher, RETEMSA

Estos dispositivos suelen ser costosos y dependiendo de su certificación de seguridad y de su velocidad varían entre 3.000 y 25.000 euros.

1.5_Seguridad física y ambiental

Objeto: Prevenir accesos físicos no autorizados a las instalaciones de la organización.

La primera acción que abordaremos dentro de la seguridad de los sistemas informáticos es su seguridad física. Habría que plantearse, donde ubicarlos y quien puede tener acceso físico a los equipos. Después deberemos poner los controles para que esta política se aplique de manera eficiente.

Los riesgos que evitaremos aplicando esta política pueden ser de carácter involuntario (alguien tropieza y tira el café que llevaba en la mano

encima del equipo) o voluntario (acto vandálico o sabotaje). Acciones ambientales, fuego, polvo, agua. Perdida de datos por emisiones radioeléctricas.

Existen multitud de dispositivos que controlan que los equipos se mantengan dentro de los límites ambientales necesarios para su buen funcionamiento. Estos dispositivos son de fácil instalación y bajo coste que pueden estar conectados a una central de alarmas. Otra posibilidad es la conexión a un equipo informático (la mayoría tienen utilidades que permiten la consulta de los datos recogidos en el dispositivo desde un ordenador) y que este nos mantenga informados a través de notificaciones vía SMS.

- **Controles ambientales:** Control de temperatura, Control de humedad y líquidos, Control de humos y gases.
- **Controles de presencia física**: Cámaras IP conectables directamente a la red de datos mediante conector físico o inalámbrico. Estas cámaras tienen posibilidad de grabar movimientos y dejarlos registrados.

Para un usuario domestico o micropyme la ubicación de los sistemas y su acceso físico es un problema menor aunque no por ello debe ser obviado. Si el equipo tiene una llave de acceso al botón de encendido deberemos usarla. El uso de contraseñas de acceso por usuario y la protección de salvapantallas con contraseña seria suficiente para evitar que alguien pueda manipular el equipo.

Siempre que se pueda debe habilitarse una sala o un espacio especial para la ubicación de los sistemas de información. Es importante que el acceso este restringido mediante una llave de entrada que puede ser física, lógica o una combinación de ambas. Si no disponemos de una habitación deberíamos tener al menos una jaula o armario cerrado.

La seguridad física se puede incrementar mediante la implantación de diferentes anillos de seguridad. Estos anillos están formados por áreas concéntricas donde la más interior será el lugar más seguro y donde se encuentre el activo mas preciado de la organización. El control en las diferentes capas será incremental, de tal forma que cada vez se necesiten más acreditaciones para acceder a capas interiores.

Los controles de acceso a los diferentes niveles o capas, como hemos comentado pueden ser de diferente naturaleza, físicos (llaves) lógicos : Tarjetas , RFID. Controles Biométricos.

Podemos encontrar en el mercado productos adaptados a la custodia de activos informáticos: Armarios ignífugos con protección radioeléctrica. Estos últimos incuso permiten instalar dispositivos de refrigeración, extinción de incendios y controles antihumedad integrados.

Sala technomovil para albergar sistemas de información

Alimentación eléctrica

Uno de los riesgos a los que tenemos que dar respuesta es la posible falta de corriente eléctrica, para ello tenemos varias soluciones dependiendo de la autonomía que queramos obtener:

1. Duplicidad de proveedores de suministro eléctrico. (Instalación complicada.)
2. UPS. Equipos de baterías autónomas. (Instalación sencilla coste elevado para altos niveles de autonomía).

3. Grupo Electrógeno. Generador de corriente eléctrica con gasoil. (Coste razonable, sin problemas de autonomía, requerimientos de instalación mas exigentes).

Comunicaciones

Garantizar las comunicaciones es una tarea fundamental para mantener nuestros sistemas accesibles. Las soluciones mas adecuadas son la utilización de distintos proveedores de comunicaciones con una infraestructura de red independiente.

Si se trata de tener acceso al exterior la configuración de dos proveedores de ADSL puede ser una opción interesante y barata. Solo tendríamos que configurar los accesos en nuestros equipos para poder acceder por cualquiera de ellos.

Cuando estamos ofreciendo servicios a terceros, la tecnología ADSL también puede resultar de utilidad. La tecnología ADSL es asimétrica mas pensada para acceder a servicios que a servir como vía para ofrecerlos, de hecho las velocidades de subida son inferiores a las de bajada. Por otro lado los contratos de servicio de ADSL no aseguran los caudales y por lo tanto podemos encontrarnos con problemas si no hemos dimensionado al alza nuestra conexión. No obstante podemos encontrar proveedores de acceso ADSL especializados que nos ofrecen servicios de valor añadido como conexiones con velocidades simétricas y con garantías de servicio pero con precios que se acercan mas a otras tecnologías de mayor estabilidad.

En el caso de ofrecer servicios es importante como hemos dicho tener más de un suministrador de acceso para cubrir el riesgo de caídas en un proveedor. La garantía de enrutamiento se realiza mediante protocolos BGP y sistema autónomo de IPs. Un proceso complicado que solo estaría al alcance de grandes empresas proveedoras de servicios. Existen sin embargo opciones menos complicadas como dispositivos balanceadores de IP que permiten la publicación de nuestras direcciones de servicio en diferentes proveedores y su gestión de tal forma que podamos ser accedidos desde caminos distintos.

También existen otras formas de mantener la disponibilidad a través de configuraciones de sistemas de DNS como Round Robin. El mecanismo consiste en configurar nuestro sistemas de DNS (Servidor de nombres donde se asocia una dirección tipo www.miempresa.com con una IP dirección

física en Internet tipo 195.76.104.6) para asignar mas de una IP a un mismo nombre. De esta forma nuestro DNS servirá distintas direcciones IPs (quizás cada una de un proveedor distinto) cada vez que se le pregunte.

Protección en equipos móviles

Cada vez mas los dispositivos móviles adquieren un mayor protagonismo. Los teléfonos, PDA´s, PC portátiles...etc. exigen una atención especial respecto a su seguridad. El uso de estos dispositivos añade nuevas amenazas como pueden ser el robo o la pérdida del dispositivo. Existen una serie de aplicativos que nos ayudaran a mejorar la seguridad de estos. Principalmente tendremos que implantar controles en las comunicaciones inalámbricas, la seguridad física para evitar robos o daños en el dispositivo, seguridad de los datos (cifrado y autenticación) y seguridad correctiva (copias de seguridad, backups).

Crypt2000 de Secuware

- Permite el arranque de la máquina con tarjeta.
- Control de Acceso
- Cifrado del Disco Duro
- Cifrado de Carpetas de Red
- Arranque con Tarjeta

TrueCrypt

- Herramientas de cifrado de disco en tiempo real mantenida bajo licencia libre y disponible en entornos Windows como Linux, podemos cifrar discos duros o particiones enteras.

Control de acceso. Smartcardlogon de Windows.

- Configuración de acceso al equipo con tarjeta criptográfica mediante acceso a Active Directory. Ver certificados digitales.

Control físico. Correas antirrobo.

- Es recomendable usar cadenas antirrobo si vamos a utilizar equipos portátiles en oficinas externas y estos van a estar en algún momento desatendidos.

Otra herramienta que permite incorporar seguridad a los dispositivos moviles es **AC Camerfirma Dfirma PDA**. Esta herramienta permite incorporar el cifrado la firma de documentos y el envío de mensajes firmados y cifrados en un dispositivo PDA.

1.6_Conformidad

Objetivo: Evitar inflingir leyes, normativas, regulaciones u obligaciones contractuales

1.7_Seguridad de recursos humanos

Asegurarse que los empleados, tanto internos como subcontratados entiendan su labor y la responsabilidad asociada así como que tengan un perfil adecuado a su función, de forma que se reduzca la probabilidad de riesgo robo o fraude.

1.8_Aspectos organitzativos para la seguridad: organización interna; organización externa

El objetivo de este capitulo del estándar es la gestión del la seguridad de la información dentro de la empresa. La gestión consiste en aprobar la política de seguridad, asignar roles de seguridad, revisar la implementación de la seguridad en la empresa asegurando una visión multidisciplinar de la gestión.

Al aplicar herramientas operativas más que técnicas no aplica a este apartado.

1.9_Gestión de activos

El objetivo es almacenar, identificar y proteger de forma apropiada los activos de la organización. Estos activos deben ser inventariados. Bases de Datos, ficheros, contratos, acuerdos, documentación de sistemas, aplicaciones de software, ordenadores, equipos de red, dispositivos de almacenamiento, equipos de comunicación, refrigeración, documentación del personal, intangibles como la reputación de la organización, marca, etc.

Al aplicar herramientas operativas más que técnicas no aplica a este apartado.

10_Plan de continuïdad y contingencias

Objetivo: Evitar interrupciones de las actividades de negocio y proteger los procesos críticos de los efectos derivados de fallos importantes en los sistemas de información o desastres y asegurar su reestablecimiento en un tiempo predeterminado.

Los beneficios de la seguridad. Casos de éxito

Josep Maria Clopés
Director de Negocio de Gematic

1_INTRODUCCIÓN

En este capítulo se recopilan diversos casos de éxito que muestran de forma práctica los beneficios que puede aportar la firma electrónica a una entidad o empresa.

Cada uno de los casos será presentado de forma individual intentando explicar de forma sencilla la complejidad del mismo y la solución aportada así como los beneficios reportados por su implantación.

Los casos han sido escogidos intentando abarcar los máximos paradigmas posibles para poder mostrar que la firma electrónica puede aportar beneficios en un gran número de situaciones, facilitando y asegurando las acciones que ahora mismo se realizan de forma telemática o incluso presencial. Se podrá observar que no solo se incluyen casos de aplicaciones web sino también de aplicaciones de escritorio con lo que se refuerza la idea de que la firma electrónica tiene un abanico de utilización muy amplio.

Los casos de éxito que se pueden encontrar en este capítulo son los siguientes:

- Adaptación del producto de gestión empresarial de Gematic, S.A. para emitir facturación electrónica.
- Desarrollo de una plataforma llamada «Oficina Virtual de Signatura de Convenis» para la Agencia Catalana de Certificació, utilizando dicha plataforma, tanto administraciones públicas como empresas que firmen convenios con ellas pueden firmar digitalmente los mismos.
- Desarrollo de una plataforma de registros de creaciones para Barcelona Centre de Disseny donde los autores pueden registrar sus creaciones garantizando de forma fehaciente que en la fecha de registro disponían de esa creación.

- Desarrollo de una plataforma de exportaciones temporales para la Cámara de Comercio de Barcelona para facilitar el trámite de exportaciones temporales a las personas físicas y jurídicas que tienen que sacar mercancía temporalmente de España, pudiendo realizar este trámite de forma no presencial.
- Banc Sabadell: Plataforma de Factura Electrónica y utilización de DNI Electrónico.
- Portic

2_CASOS DE ÉXITO

A continuación se presentan los diferentes casos de éxito. En cada uno de ellos se presentarán sus particularidades.

2.1_Adaptación de producto de gestión empresarial

Presentación del caso

Este caso de éxito quizás es el típico caso que se puede aplicar a la mayoría de las empresas. Se centra en la facturación electrónica que posiblemente sea la casuística más conocida de las que se solucionan utilizando la firma electrónica. Esto es debido a que es la más universal ya que en todas las empresas se factura y es la más sencilla de exponer tanto a nivel de funcionamiento como de beneficios económicos

La facturación electrónica se aplica en todo tipo de empresas y su fin es el mismo en todas ellas: agilizar procesos, ahorrar dinero, garantizar la seguridad de los trámites, convertir un trámite engorroso y largo en una operación cómoda, sencilla y fiable.

Las ventajas aportadas por la implantación del sistema son las siguientes:

- Evita el gasto de impresión porque las facturas se envían en formato electrónico
- No acumula papel. Las facturas electrónicas se pueden guardar en CD o en el disco duro del ordenador

- Una factura electrónica no puede modificarse. Para firmar se requiere un certificado digital reconocido por la Agencia Tributaria. El certificado garantiza que el documento no ha sido modificado
- Sólo se necesita un certificado digital y la herramienta que permite firmar electrónicamente desde un ordenador

Control de accesos

El control de accesos al sistema está controlado por el módulo estándar del producto de gestión empresarial denominado SKX. Este permite gestionar altas, bajas y modificaciones de usuarios así como las funcionalidades a las que puede acceder un usuario y con que permisos.

Por ejemplo, se puede definir si un usuario puede acceder a la opción de facturación y si puede acceder con permisos de consulta o modificación.

Además los usuarios tienen el password cifrado y el usuario inicial de conexión usado solo tiene permiso de selección de datos sobre la tabla de usuarios para que nadie pueda acceder a los datos sin usar producto el SKX.

Desarrollo y mantenimiento del sistema

El desarrollo del sistema se basa en la modificación de un producto existente para que realice parte de las tareas que realizaba hasta el momento añadiendo la facturación digital al proceso.

Como toda herramienta de gestión empresarial, el producto SKX ya disponía de proceso de facturación. La solución se centra en modificar el proceso para que sea lo más genérico posible y permita a toda empresa acceder a este nuevo mundo de la firma digital de la forma más sencilla posible.

La facturación digital se puede llevar a cabo con diferentes niveles de complejidad. Como la finalidad del proyecto era facilitar la utilización de este tipo de tecnología al mayor número de personas garantizando la veracidad y integridad de la información, se escogió sustituir la factura en soporte papel por factura en formato PDF. De esta manera, la gran mayoría de empresas pueden trabajar con ella sin necesidad de desarrollos especiales en sus sistemas y permitiendo que puedan visualizarla de forma sencilla, confiando de esta manera en el proceso.

Evidentemente, con las premisas comentadas anteriormente, el proceso debe ser muy sencillo y como tal se resume en los siguientes pasos:

1. Elaboración de la factura en el ordenador utilizando el proceso de facturación del producto SKX.
2. Conversión de las facturas a formato PDF.
3. Firma de las facturas utilizando el certificado digital del usuario.
4. Envió de las facturas mediante correo electrónico al destinatario definido en el sistema.
5. El receptor solo debe abrir la factura en formato PDF con el lector de Adobe y automáticamente visualiza la factura con la firma y su validación (siempre y cuando el software esté correctamente configurado).

En el siguiente diagrama se pueden ver de forma gráfica los pasos a seguir.

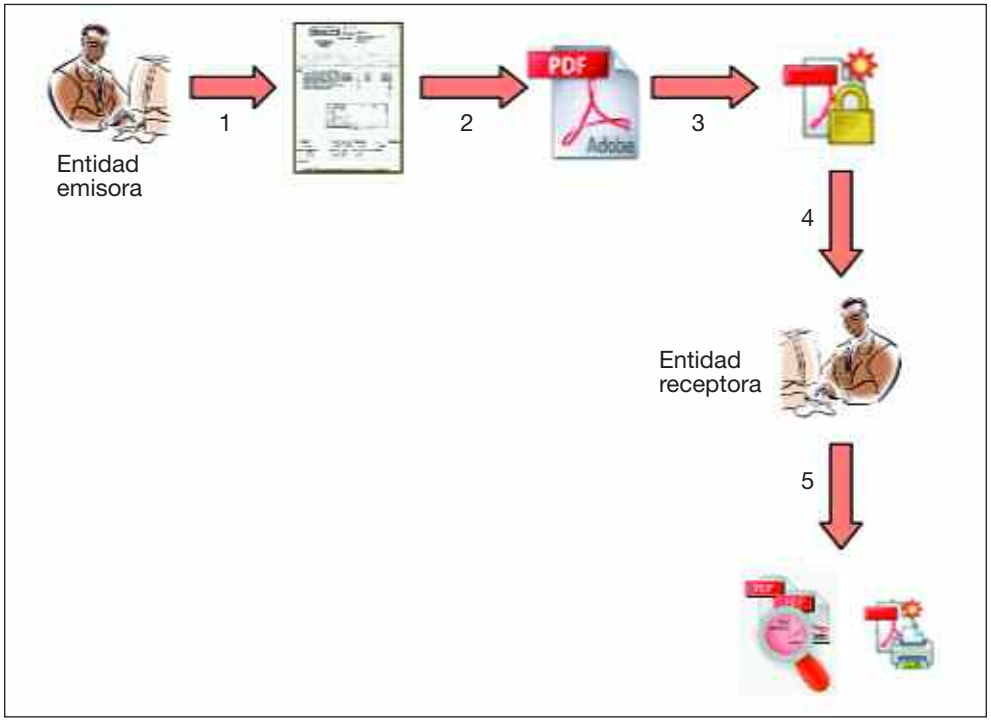


Diagrama de proceso de facturación electrónica.

Conformidad legal

Según la legislación actual1, la conformidad legal del proceso presentado se basa en las siguientes bases legales:

- La factura electrónica tiene la misma validez legal que la factura de papel.
- Cualquier persona física o jurídica puede facturar electrónicamente.
- Para facturar se requiere un certificado digital reconocido por la Agencia Tributaria.

Haciendo que el proceso esté amparado por la ley.

2.2_Plataforma «Oficina Virtual de signatura de convenis»

Presentación del caso

El objeto de este caso de éxito es el desarrollo e implantación de una plataforma web de firma electrónica de convenios (documentos en formato PDF) para la Agencia Catalana de Certificació.

Esta plataforma permite gestionar todo el circuito de un convenio desde la carga inicial del documento en la plataforma, el acceso de los diferentes actores al proceso y la firma del documento utilizando la propia plataforma.

La idea central del proceso es sustituir el procedimiento manual de la firma de documentos por un procedimiento no presencial, con la ventaja que ello conlleva. Si pensamos en un documento que deba ser firmado por personas que estén localizadas en diferentes zonas geográficas se pueden eliminar los desplazamientos de las personas que deben firmar y además se elimina la dificultad de encontrar una fecha en la que todas las personas que deben firmar tengan disponibilidad.

Esto es debido a que con este sistema, no es necesario que las personas que tienen que firmar un documento estén en la misma sala ni en el mismo instante, cada una puede firmarlo en su localidad y de forma inmediata sin necesidad de conciliar agendas con otras personas.

Las ventajas aportadas por la implantación del sistema son las siguientes:

- Evita el gasto de impresión de documentos puesto que el documento firmado solo es válido en formato electrónico y por tanto no se imprime.
- No acumula papel. Los documentos a firmar se almacenan en la plataforma y cada persona puede almacenarlo en un CD o disco duro.

- El documento no puede ser modificado. Para firmar se requiere un certificado digital reconocido. El certificado garantiza que el documento no ha sido modificado
- Solo se necesita un certificado digital reconocido y acceso a Internet para poder firmar documentos
- No es necesario el desplazamiento de las personas a una localización común para realizar la firma.
- No es necesaria la conciliación de agendas para firmar el documento.

Control de accesos

El acceso a la plataforma se debe realizar de forma obligatoria utilizando un certificado digital válido. Dicho control de acceso se valida utilizando la Plataforma de servicios de identificación y firma (PSIS). El objetivo de esta plataforma es entre otros la validación de firmas digitales.

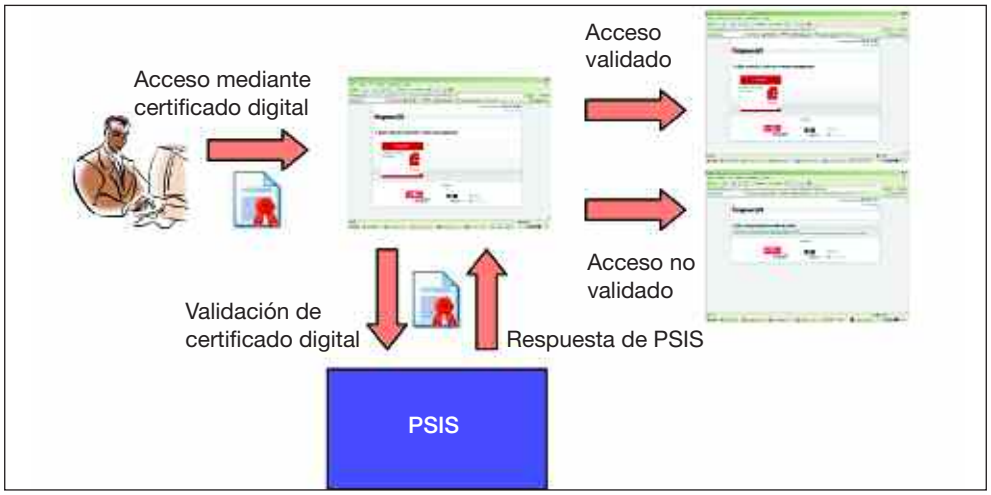


Diagrama de proceso de validación de firmas.

Como se puede ver en el diagrama anterior, la aplicación se comunica con PSIS y le envía la información del certificado digital de la persona que intenta conectarse. PSIS contesta con la validación correcta o incorrecta de dicha información. Con ello nos aseguramos que la persona que está accediendo tiene una firma digital válida.

Además, dicha persona debe tener permiso para acceder a la plataforma, esto es gestionado por un módulo de seguridad que permite altas, bajas y modificaciones de usuarios así como los accesos a los que puede acceder el usuario.

Si a todo esto se le suma la seguridad que añade la utilización de un certificado digital, que nos garantiza que la persona que está conectándose es realmente quien dice ser, cerramos el círculo de seguridad.

Desarrollo y mantenimiento del sistema

Como se comenta en la presentación del caso, la plataforma está basada en sistema web. Esto significa que es accesible desde cualquier ordenador con conexión Internet permitiendo la utilización de la plataforma sin la necesidad de instalar ningún tipo de software en el ordenador.

Para poder conseguir que las personas que deben firmar los documentos pudieran utilizar la plataforma se definieron ciertas premisas que se la plataforma debía poder controlar:

- Desarrollar una plataforma que tenga un uso muy sencillo
- Poder definir las personas que tienen acceso a la misma
- Poder publicar en ella los documentos a firmar
- Poder definir las personas que deben firmar un documento
- Poder definir y controlar el orden de firmas del documento
- Avisar a los implicados de los documentos a firmar
- Validar las firmas de los implicados
- Integrar la información con el gestor documental corporativo

En el siguiente diagrama se representan los pasos que hay que realizar para poder firmar un documento utilizando la plataforma.

Como se puede ver en el diagrama anterior, los pasos para realizar una firma son sencillos e intuitivos:

1. Cargar el documento el la plataforma y definir las personas que deben firmarlo y el orden. El documento puede ser cargado a partir del gestor documental o a partir de un equipo local.
2. El sistema automáticamente avisa al primer usuario de que tiene un documento para la firma.
3. El primer usuario accede a la plataforma y firma el documento.
4. El sistema avisa automáticamente al siguiente usuario de que tiene un documento pendiente de firma.

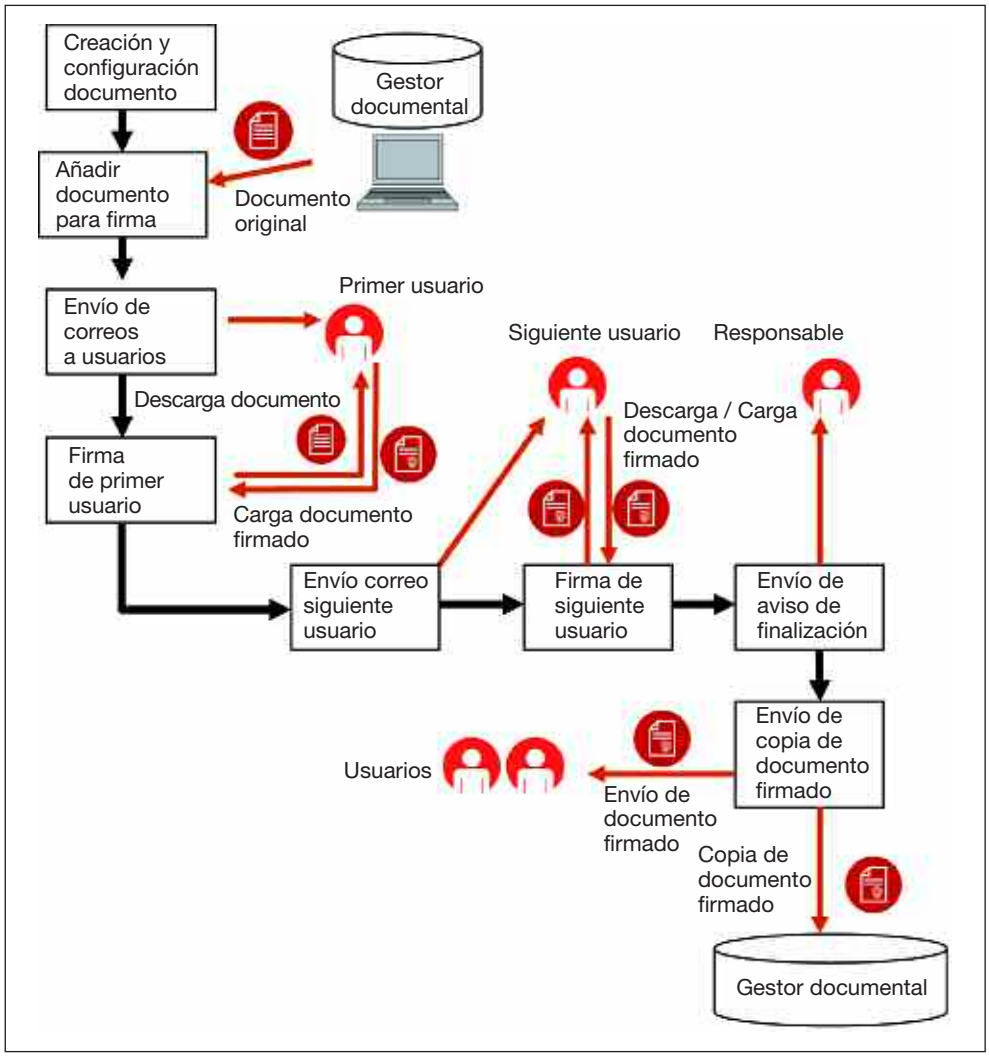


Diagrama de circuito estándard de firma de un documento.

5. El siguiente usuario accede a la plataforma y firma el documento.
6. Los puntos 4 y 5 se repiten hasta que hayan firmado todos los implicados y en ese momento el sistema avisa de que se ha finalizado el proceso y envía una copia del documento firmado por todos a todos los implicados además de almacenar una copia del mismo en el gestor documental.

Seguridad física y del entorno

La aplicación es accesible utilizando HTTPS.

El sistema HTTPS utiliza un cifrado basado en las Secure Socket Layers (SSL) para crear un canal cifrado más apropiado para el tráfico de infor-

mación sensible que el protocolo http, que es el protocolo estándar usado para la navegación por Internet.

Esto garantiza que la información intercambiada entre el usuario que se conecta a la aplicación y la aplicación no puede ser visualizado por un tercero.

Además de esto, el sistema está alojado en servidores que tienen las medidas de seguridad estándar de servicio web de alta disponibilidad, garantizando que el acceso físico a los mismos está estrictamente controlado.

Conformidad legal

Según la legislación actual, la conformidad legal del proceso presentado se basa en las siguientes bases legales:

- La firma digital de nivel reconocido puede sustituir legalmente a la firma manuscrita. Por tanto cualquier documento electrónico firmado con ella tiene el mismo valor que un documento firmado manuscritamente sobre papel.

2.3_Plataforma de registro de creaciones

Presentación del caso

El objeto de este caso de éxito es el desarrollo e implantación de una plataforma web de registro de diseños para Barcelona Centre de Disseny.

El objetivo de la plataforma es aportar a los autores de creaciones una herramienta para dilucidar la propiedad de una creación.

Para ello, la plataforma permite a los autores de ideas registrarlas utilizándola (cargar documentos electrónicos en la misma) y permitiendo de esta manera demostrar que en la fecha de registro el autor disponía de dicha idea en su poder. Para ello utiliza un sellado de tiempo que garantiza que dicho documento se cargó en la plataforma en dicha fecha y que no ha podido ser modificado.

De esta manera, en el caso de que se produzca una diferencia de criterios en la propiedad de una creación, el autor que haya utilizado la plataforma puede demostrar la fecha en que la cargó en ella y que desde entonces el documento no ha podido ser modificado.

Las ventajas aportadas por la implantación del sistema son las siguientes:

- Permite a los autores presentar una prueba de que disponían de una creación en su poder en una fecha de forma fehaciente.
- Permite a los autores mostrar a sus clientes un número de registro de la plataforma para evitar que dicha idea o creación pueda ser usada sin pagar por ella.
- Evita tener que hacer otros tipos de registro que se hacían hasta el momento como por ejemplo auto enviarse sobres certificados con las creaciones dentro o acudir al notario para que almacene sobres cerrados conteniendo las creaciones.
- El documento no puede ser modificado. Para acceder a la plataforma se requiere un certificado digital. El certificado garantiza que el documento no ha sido modificado
- Solo se necesita un certificado digital y acceso a Internet para poder registrar creaciones.
- No es necesario el desplazamiento de las personas a un notario o a correos para proteger sus creaciones.

Control de accesos

El acceso a la plataforma se debe realizar de forma obligatoria utilizando un certificado digital válido de diferentes entidades de certificación reconocidas por la Agencia Tributaria.

De esta forma se garantiza la identidad del usuario que accede a la misma.

Para poder garantizar la validez del certificado se realizan diferentes acciones:

- Comprobar que el certificado está expedido por una entidad de certificación valida (Camerfirma, CATCert, Firmaprofesional, Autoridad de Certificación de la Abogacía, Agencia Notarial de Certificación, ANF Autoridad de certificación, Izempe, Servicio de certificación de los Registradores, etc)
- Comprobar que el certificado no ha caducado (todo certificado dispone entre sus datos de su fecha de fin de validez)
- Comprobar en las CRL (Certificate Revocation List o lista de revocación de certificados) que el certificado no ha sido revocado.

Una CRL es una lista de certificados (más concretamente sus números de serie) que han sido revocados, ya no son válidos y en los que no debe confiar ningún sistema de usuario.

En el siguiente diagrama se puede ver gráficamente el proceso de validación de certificados en el acceso a la plataforma

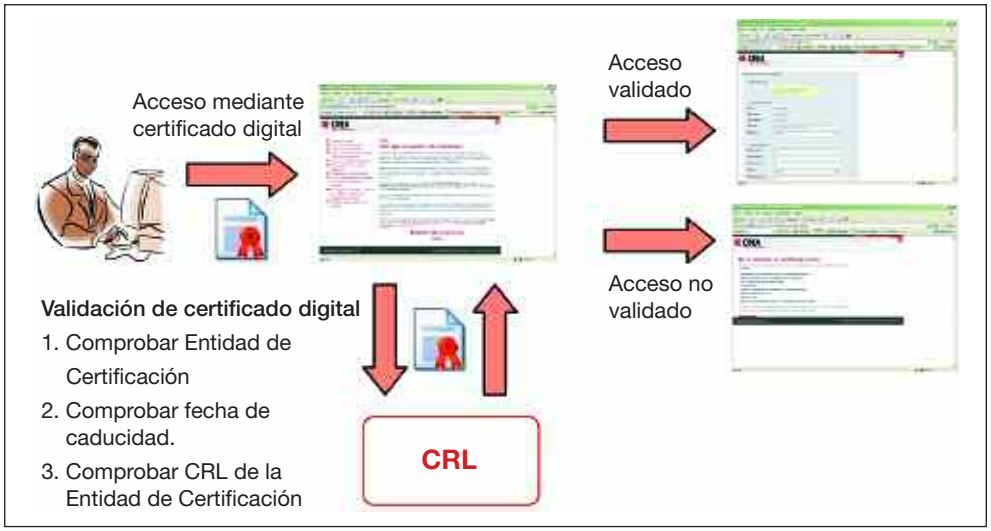


Diagrama de proceso de validación de certificados.

Desarrollo y mantenimiento del sistema

Como en otros casos presentados, la plataforma está basada en sistema web. Esto hace que haya algunas características parecidas, como por ejemplo, que es accesible desde cualquier ordenador con conexión Internet permitiendo la utilización de la plataforma sin la necesidad de instalar ningún tipo de software en el ordenador.

Para garantizar la consecución de los objetivos de la plataforma se definieron las siguientes funciones como puntos clave:

- Desarrollar una plataforma que tenga un uso muy sencillo
- Poder definir las personas que tienen acceso a la misma
- Poder replicar la instalación en otras Camaras.
- Impresión de los cuadernos oficiales desde la propia aplicación
- Gestión de las incidencias de los cuadernos
- Integración con la solución de gestión empresarial corporativa.
- Integración con TPV Virtual

En el siguiente diagrama se representan las interacciones entre los diferentes actores.

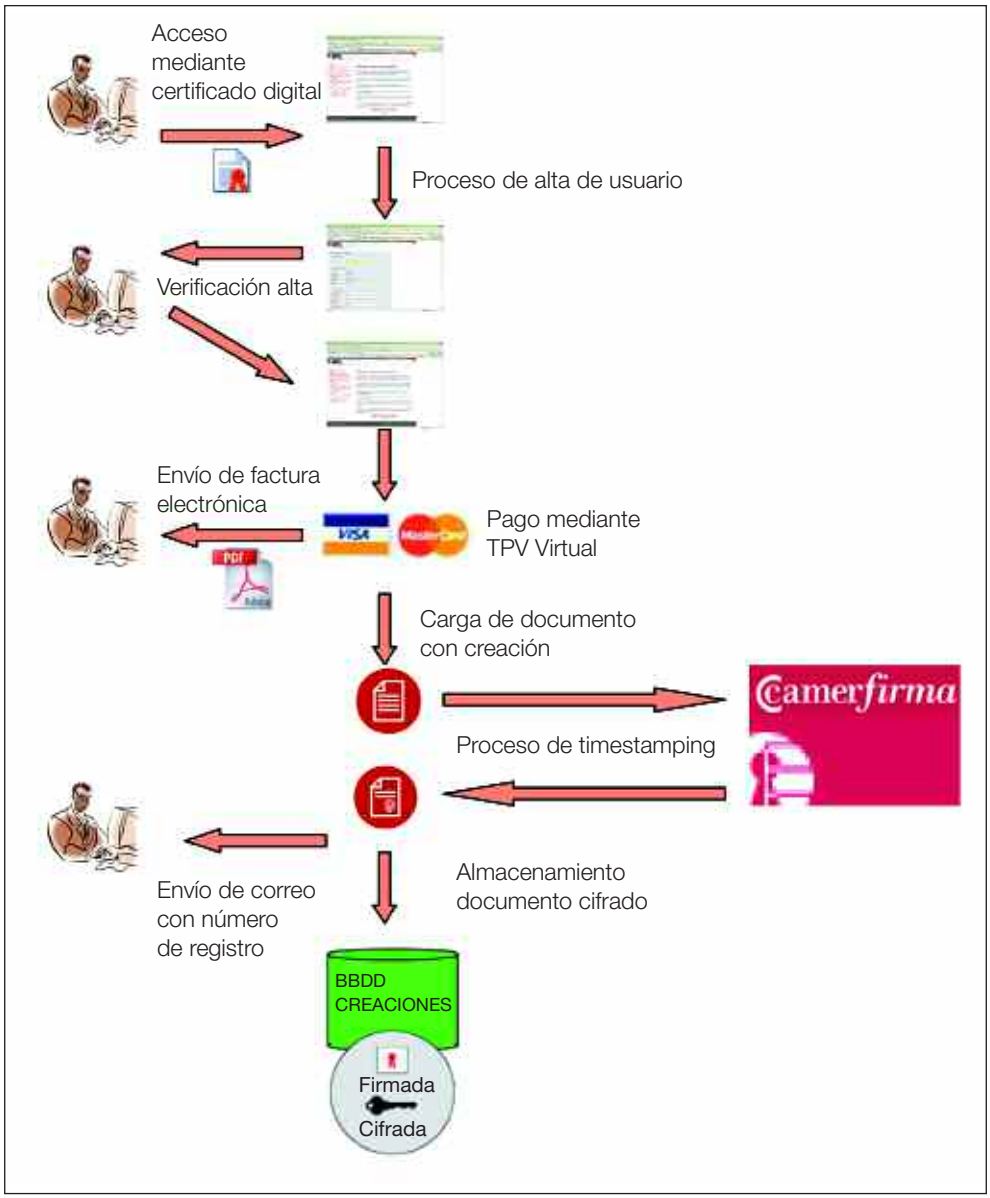


Diagrama de proceso del registro de una creación.

En el diagrama actual se puede ver el proceso de un registro de creación:

1. Registrarse en la plataforma.
2. Comprar bonos de registro mediante TPV Virtual.
3. La plataforma emite factura electrónica

4. Cargar el documento en la plataforma
5. El sistema realiza el proceso de sellado de tiempo mediante el servicio de Camerfirma
6. El sistema cifra el fichero y lo almacena. Además el sistema envía un correo de confirmación con número de registro.

Seguridad física y del entorno

La aplicación es accesible utilizando HTTPS.

El sistema HTTPS utiliza un cifrado basado en las Secure Socket Layers (SSL) para crear un canal cifrado más apropiado para el tráfico de información sensible que el protocolo http, que es el protocolo estándar usado para la navegación por Internet.

Esto garantiza que la información intercambiada entre el usuario que se conecta a la aplicación y la aplicación no puede ser visualizado por un tercero.

Además de esto, el sistema está alojado en servidores que tienen las medidas de seguridad estándar de servicio web de alta disponibilidad, garantizando que el acceso físico a los mismos está estrictamente controlado.

Conformidad legal

Según la legislación actual, la conformidad legal del proceso presentado se basa en las siguientes bases legales:

- La firma digital identifica de forma inequívoca y garantiza el no repudio.
- El sello de tiempo, además de garantizar la exactitud de la información temporal generada, garantiza que el documento no ha podido ser modificado desde su generación.

2.4_Plataforma de exportaciones temporales

Presentación del caso

Las Cámaras de Comercio gestionan la emisión de cuadernos ATA, los cuales se tienen que presentar en las aduanas para las exportaciones / importaciones de mercancías durante un periodo temporal.

El desarrollo de este sistema de información, permite la creación de cuadernos ATA por parte de la Cambra de Barcelona sobre un entorno web.

Además permite la identificación de los usuarios utilizando certificado digital, permitiendo de esta manera que realicen muchas de las gestiones desde la oficina.

Las ventajas aportadas por la implantación del sistema son las siguientes:

- Evita los desplazamientos del representante de la empresa o ciudadano.
- Elimina las colas en el mostrador.
- Gestión integral de todo el circuito de un cuaderno ATA.

En el siguiente diagrama se refleja la diferencia entre los desplazamientos que debe realizar un representante antes y después de disponer de la plataforma:

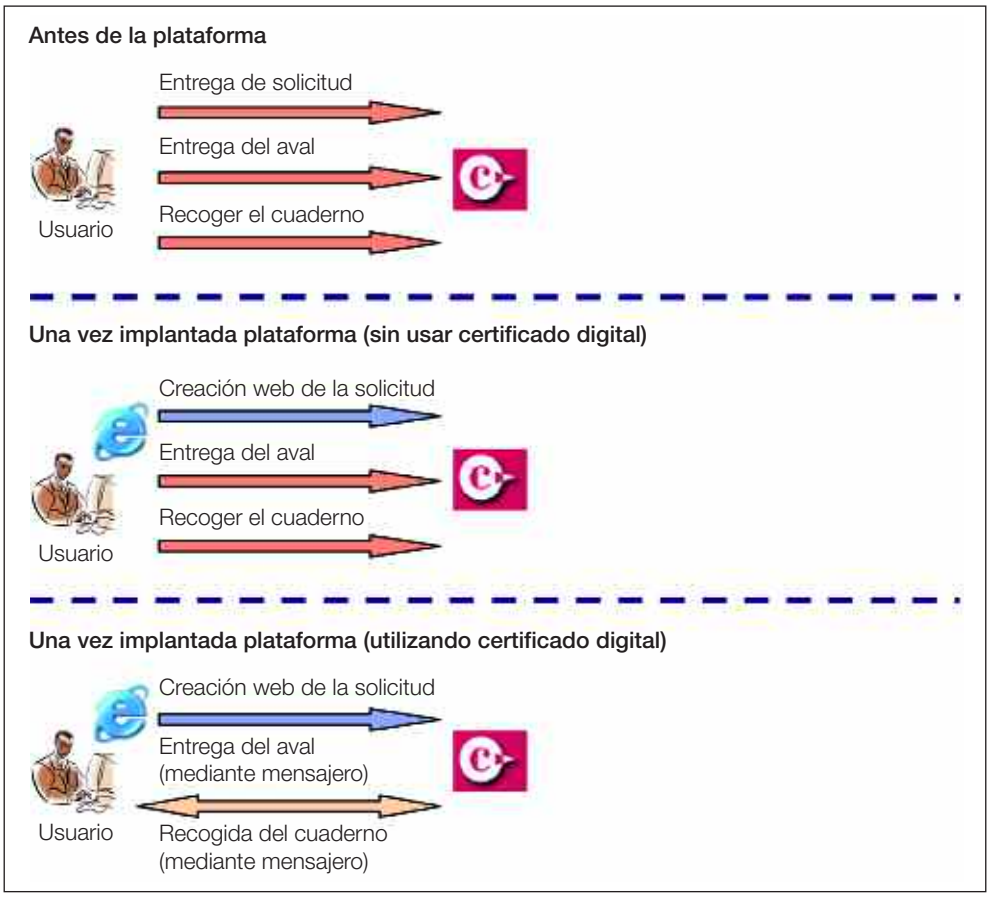


Diagrama de proceso de validación de certificados.

Como se puede ver en el diagrama anterior, los viajes realizados por el usuario con el sistema tradicional o con la nueva plataforma se reducen sustancialmente los desplazamientos. Inicialmente se pueden ver hasta tres viajes solo para conseguir el cuaderno. Con la nueva plataforma, el usuario puede pedir que un mensajero recoja el aval en su domicilio, lo entregue en la Cámara de Barcelona, recoja el cuaderno y lo entregue. Si a eso sumamos la solicitud online se consigue eliminar el desplazamiento totalmente.

Control de accesos

El acceso a la plataforma se debe realizar de forma obligatoria utilizando un certificado digital válido de Camerfirma.

De esta forma se garantiza la identidad del usuario que accede a la misma.

Además, el sistema permite definir usuarios y los accesos a las funcionalidades a las que cada uno tiene permiso de acceso.

Desarrollo y mantenimiento del sistema

La plataforma está enfocada a la gestión total de los cuadernos de exportación temporal (ATA en la mayoría de los casos aunque también hay otro tipo minoritario llamado CPD).

El sistema gestiona todo el circuito de estados de cuaderno desde su solicitud hasta su entrega en las oficinas de la Cámara de Barcelona después de su uso. Incluso después de dicha entrega se pueden gestionar incidencias de las aduanas, que evidentemente llegarán más tarde que el susodicho cuaderno.

En el siguiente diagrama se puede apreciar el circuito gestionado por la plataforma:

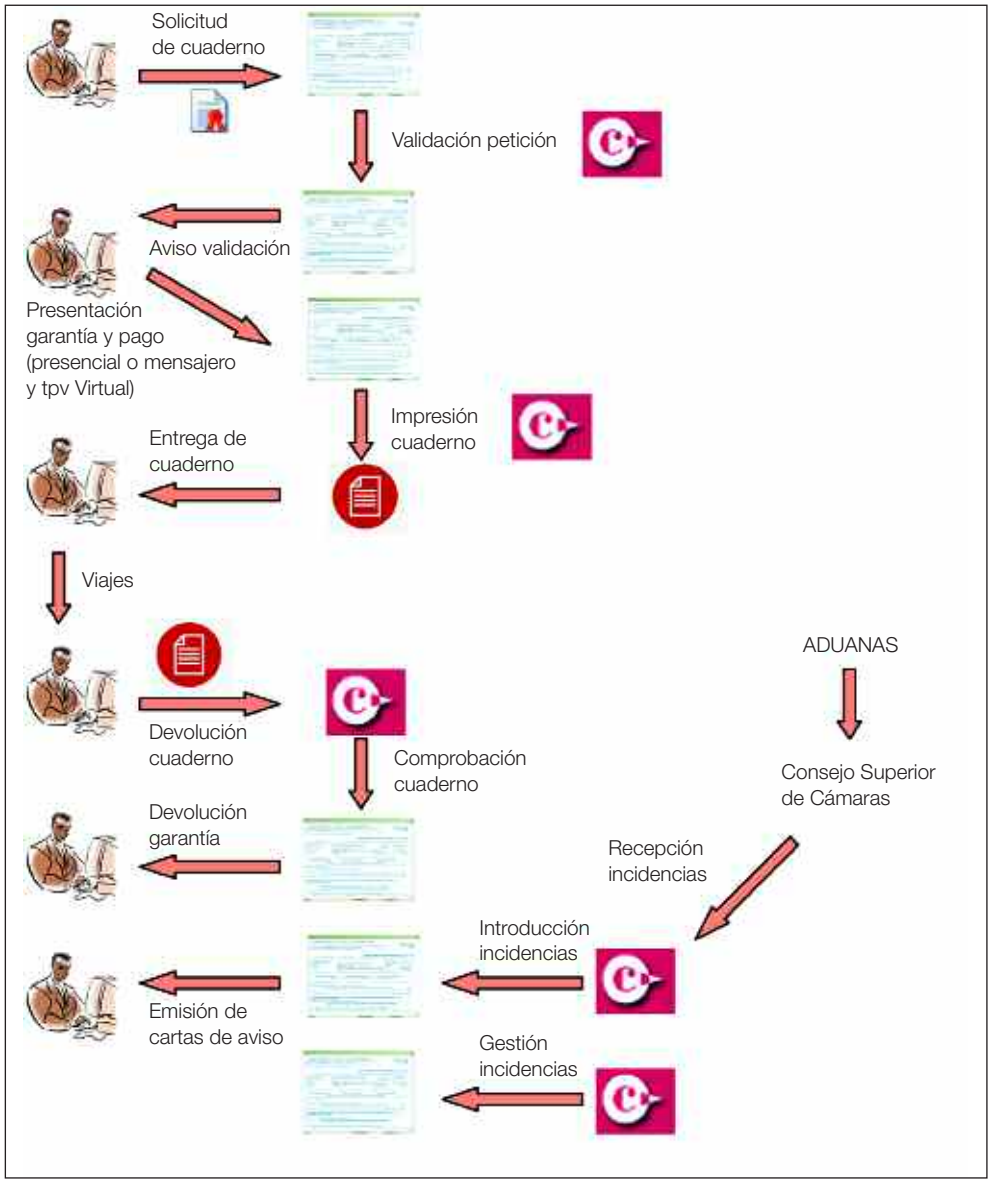


Diagrama de proceso de la gestión de un cuaderno

Seguridad física y del entorno

La aplicación es accesible utilizando HTTPS.

El sistema HTTPS utiliza un cifrado basado en las Secure Socket Layers (SSL) para crear un canal cifrado más apropiado para el tráfico de información sensible que el protocolo http, que es el protocolo estándar usado para la navegación por Internet.

Esto garantiza que la información intercambiada entre el usuario que se conecta a la aplicación y la aplicación no puede ser visualizado por un tercero.

Además de esto, el sistema está alojado en servidores que tienen las medidas de seguridad estándar de servicio web de alta disponibilidad, garantizando que el acceso físico a los mismos está estrictamente controlado.

Conformidad legal

Según la legislación actual, la conformidad legal del proceso presentado se basa en las siguientes bases legales:

- La firma digital identifica de forma inequívoca y garantiza el no repudio.

2.5_Plataforma de Factura Electrónica: BS Factura

Presentación del caso

Banc Sabadell fue la primera entidad Bancaria que, a finales del año 2006, reconoció el DNI Electrónico adaptando sus procesosde negocio para que sus clientes pudieran identificarse mediante esta acreditación al utilizar los servicio de su portal Internet.

En el caso de la factura electrónica, su andadura comienza en el año 2000 con la creación de una Joint Venture con Siemes para la creación de una plataforma dirigida, inicialmente, a dos tipos de clientes:

- **Gran emisor:** Empresas que por su tipología y volumen de negocio generarn una gran cantidad de facturas a clientes (Como por ejemplo: Iberia, Gas Natura, etc.)
- **Gran receptor:** Es el caso complementario al anterior, donde las empresas reciben una gran cantidad de facturas (Ejemplo: El Corte Inglés, BonPreu, etc.).

Actualmente, la plataforma de factura electrónica se encuentra operativa e integrada en el catálogo de productos del Banco, como un producto más del portfolio que los gestores comerciales ponen a disposición de sus clientes. Existen dos posibles niveles de utilización de la plataforma:

- **Bàsico:** en términos sencillos, permite a cualquier cliente el intercambio de ficheros electrónicos con el portal para la recepción generación de facturas.

- **Integrado:** Se realiza una integración con la aplicación de gestión utilizada por el cliente para la emisión / recepción de facturas. De esta forma el proceso es automático y transparente (no obliga al cliente a realizar ningún proceso o tarea fuera de las habituales).

Control de accesos

El acceso a la plataforma se debe realizar de forma obligatoria utilizando un certificado digital (que varía en función de la operativa a realizar) y actualmente se está trabajando para poder aceptar cualquier certificado emitido por Autoridades de Certificación Reconocidas.

Además, el sistema permite definir usuarios y los accesos a las funcionalidades a las que cada uno tiene permiso de acceso.

Desarrollo y mantenimiento del sistema

La plataforma está totalmente integrada en el Back-Office del Banco como un producto más y permite su utilización conjunta con otros productos / servicios (Factoring, Confirming, etc.) lo que posibilita una oferta flexible y amplia de servicios integrados a disposición de los clientes.

Seguridad física y del entorno

- Factura electrónica en XML 2.0
- Firma de XMLs PKCS7 mediante certificados digitales de FNMT, CamerFirma y Firmaprofesional.
- Integración con EDI para descarga de factura electrónica.
- BSFConnector: envío y recepción de facturas vía WebDav (https)
- BSFactura implementado sobre Framework ZK → framework de aplicaciones web en AJAX, LiveData, Prefetch, Webservices, Instrumentación JMX. Integración con Sitemesh
- Integración de la plataforma con portales de clientes mediante capa webservice con traspaso de sesión.

Conformidad legal

Desde el punto de vista legal, se cumplen todos los requisitos normativos actuales y los estándares CC/UBL.

2.6_Plataforma Factura Telemática de Portic

Presentación del caso

La factura telemática, conjuntamente con los procesos aduaneros de importación y exportación, forman parte de la apuesta realizada por la mejora de la competitividad de la logística portuaria de Barcelona mediante una plataforma que mejore la interacción entre ellas.

El sistema desarrollado por Portic para la factura telemática se basa en el formato definido de factura estándar EDIFACT INVOICE DEFINIDO POR EL forum Telemático.

Portic proporciona los medios para realizar el firmado, tiem stamp y almacenamiento de datos para su posterior utilización en la aplicación de pagos.

La factura obtenida puede enviarse al receptor de dos formas:

- **Mediante correo electrónico:** fichero original firmado, PDF de la factura (firmado y con un link a un servicio de validación y acuse de recibo).
- Aquellas empresas que tengan el sistema Portic pueden recuperar, validar y transformar la factura a otro formato en caso de ser necesario.

Control de accesos

El acceso a la plataforma se realiza utilizando un certificado de usuario de Clase 2 CA de la FNMT.

Como en todos los casos de Plataforma electrónica, el acceso a los usuraos internos se define mediante un sistema de usuarios y perfiles, con determinación de las funcionalidades a las que cada uno tiene permiso de acceso.

Desarrollo y mantenimiento del sistema

La factura telemática está en proceso de implantación en el 2007 y ya permite su utilización por parte de las empresas.

Seguridad física y del entorno

- Módulo cliente aplicación Portic (BBDD local) utilizando un Java Connector para establecer una conexión SSL (recepción y envío de facturas).

- Front-End Apache 1.3.27
- LDAP 4.13
- Servidores de Aplicaciones Tomcat
- Bases de Datos Oracle 8i (almacenamiento de facturas enviadas)
- Firma de XMLs PKCS7 mediante certificados digitales de FNMT
- Integración con EDI para descarga de factura electrónica.

Conformidad legal

- Cumple con todos los estándares y normativas legales requeridos.

La seguridad a la hora de hacer negocios por Internet

Fernando de la Cuadra
Panda Security

Hace un par de decenas de años, la seguridad informática en una empresa pequeña o mediana era simplemente evitar que alguien se acercara al teclado del único ordenador, si lo había. Bastaba con cerrar con llave el despacho, o los sistemas más avanzados consistían en una llave que desconectaba el teclado.

Poco más tarde, los virus empezaron a desarrollarse y los usuarios se vieron expuestos a una amenaza para la que no estaban preparados. La tecnología no servía, y hubo que desarrollar programas que fueran capaces de detener a los virus: los «antivirus».

De nuevo, la «seguridad» pasaba a tener una nueva dimensión. Ya no solo bastaba con proteger físicamente el ordenador (o los ordenadores) contra su uso indebido por parte de personas: había que proteger la información contra su uso indebido por parte de otro tipo de información, los programas maliciosos.

Pero a la hora de integrar los procesos de negocio en Internet, nos encontramos que los sistemas informáticos que hasta entonces funcionaban en un pequeño entorno, la red local, pasaban a formar parte de una red mucho mayor, Internet, y estaban conectados a millones de ordenadores más.

Esto facilita el negocio, sin duda, pero entraña una serie de peligros muy graves. Los riesgos de un ordenador encendido y conectado a Internet son múltiples, y muchos se salen del ámbito de este libro. Baste pensar que es un dispositivo que tiene dentro de él unos circuitos eléctricos que funcionan a 220 voltios, suficientes para propinar un buen calambrazo a una persona. Y que pesa sus buenos kilogramos, suficientes para causar una herida en un pie en caso de caída o una lesión lumbar al que lo transporta. Y obliga a los usuarios a concentrar la vista en un punto brillante y a adoptar unas posturas que pueden desembocar en lesiones, muchas de ellas tipificadas como enfermedades profesionales. Pero

como decíamos, eso son cuestiones más propias de prevención de riesgos laborales que de seguridad informática propiamente dicha.

La seguridad informática no consiste en hacer que un sistema informático no tenga riesgos, sino que esté suficientemente protegido para los riesgos a los que se enfrenta. El peligro está ahí, y no puede evitarse. Lo que hay que hacer es evitar que ese peligro se manifieste en forma de catástrofe en el ordenador.

¿Es peligroso cruzar una calle? Por supuesto, pero para que ese peligro quede mitigado y reducido a la mínima expresión, existen semáforos. De esta manera, ¿podremos afirmar que es seguro cruzar una calle por un semáforo? Es más seguro que hacerlo por mitad de una gran avenida, por supuesto, pero es necesario que los coches estén detenidos, y que mientras crucemos sigan detenidos, y que el suelo no escurra, y que no se caiga encima de nosotros una farola, y que no haya un bache que nos haga torcernos un tobillo… Sin embargo todos los días cruzamos una calle con la confianza de que lo hacemos correctamente y que es la manera más segura.

1_ENTONCES, ¿QUÉ ES LA SEGURIDAD INFORMÁTICA?

En un sistema informático, la seguridad consiste en aplicar las medidas necesarias para que los riesgos a los que se enfrenta queden minimizados. Los riesgos nunca pueden ser eliminados, existen y nunca dejarán de aparecer nuevos peligros cada día. La seguridad informática se encarga de evitar que afecten a los sistemas, y en caso de que afecten, que su impacto sea mínimo, y en caso de que su impacto sea elevado, las medidas de seguridad harán que los sistemas vuelvan a funcionar lo más rápido y eficientemente posible.

En principio, la tarea puede parecer difícil, pero no lo es tanto. En el mundo de la informática, al igual que se han creado amenazas se han ha conseguido crear las soluciones para los mismos, aunque cada cierto tiempo aparezcan rumores de grandes catástrofes que pueden hacer perder todos los datos de un sistema.

Para cada tipo de amenaza se han desarrollado herramientas y sistemas que pueden contrarrestarla, o por lo menos, minimizar el impacto. Cada riesgo tiene sus características específicas, y debe considerarse una solución apropiada para contrarrestarla.

2_TIPOS DE AMENAZAS

Vamos a considerar que existen tres tipos fundamentales de amenazas, aunque podrían subdividirse en muchas más, pero sería un compendio excesivamente técnico:

- Amenazas por software o malware
- Amenazas de personas
- Amenazas por datos

2.1_Amenazas por software

Este tipo de peligros es lo que se ha dado en llamar «malware», palabra que proviene de la unión de «software» (programa informático, en inglés) y «malicious», malicioso. Así, el malware es el software malicioso, programas que han sido diseñados por personas que quieren causar algún perjuicio en los ordenadores o en las personas que los usan.

Dentro de esta categoría están los famosos virus informáticos. Más aún, en general se les llama virus a todos los ejemplares de malware, por extensión. En realidad, los virus no son más que uno de los tipos de malware.

Existen tres tipos básicos de malware: los virus, los gusanos y los troyanos. A partir de ellos se han desarrollado los demás, que en el fondo no son más que variaciones o cruces entre tipos de malware.

Los virus son programas que se aprovechan de otros programas para hacer copias de sí mismos. Por lo general, incorporan una serie de funciones que causan alguna molestia, desde un simple mensaje (que en ocasiones es humorístico) hasta llegar a destruir datos dentro de un ordenador.

Hay numerosos tipos de virus, en función de dónde llevan a cabo la infección (de boot, de fichero, etc.), según su forma de actuar (residentes, de acción directa…), según el tipo de fichero que infectan… Los tipos son muchos y variados.

Los troyanos o caballos de Troya son programas que se instalan sin conocimiento del usuario en los ordenadores y son capaces de llevar cabo múltiples acciones, como abrir puertas traseras, robar datos confidenciales, etc.

El nombre se emplea por su similitud con la leyenda del caballo de Troya. A los tirios se les ocurrió un truco para poder superar las murallas de Troya: fabricaron un enorme caballo de madera e introdujeron soldados dentro. Al ver el caballo, los troyanos lo introdujeron en la ciudad y los tirios, escondidos, aprovecharon para salir y conquistaron la ciudad.

Los troyanos tienen una diferencia fundamental con respecto a los virus: no infectan ficheros para propagarse por sí mismos. Si en un sistema encontramos un troyano, ha sido por una acción directa de una persona o de otro software. Ahora bien, los ejemplares puros de un determinado malware ya no se encuentran prácticamente: los desarrolladores combinan las amenazas para hacerlas más efectivas. Así, un troyano puede tener capacidad para infectar, o un virus puede tener características de troyano.

Bajo el término de troyano pueden englobarse numerosos tipos de malware, que si bien en muchas clasificaciones aparecen como una categoría aparte, al tener un componente básico de ocultación y espionaje, preferimos incluirlos en este apartado, como son el Spyware (Programas que recopilan datos sobre los hábitos de navegación, preferencias y gustos del usuario), adware (muestran publicidad), rootkits (llevan a cabo las tareas que tiene programadas sin poder detectarse fácilmente), dialers (reemplazan el sistema de conexión a Internet por módem) o los «Bots» (permanecen instalados en un sistema esperando órdenes del exterior)

Por último, los gusanos son códigos cuya única intención es propagarse a distintos ordenadores y, a diferencia de los virus, utilizando sus propios medios. Su misión es colapsar redes. Al igual que lo comentado anteriormente sobre los troyanos, hoy en día los gusanos «puros» no son habituales, ya que suelen incluir funciones adicionales que los convierten en tipos mixtos.

Como resumen de los tres grandes tipos de códigos maliciosos clásicos, esta tabla muestra sus características fundamentales:

Tipo	Propagación	Daños	Desinfección
Virus	Infectando ficheros	Sí, en el propio código	Eliminando el código del fichero infectado
Troyano	Manual, por parte de un hacker	Ninguno en su código, los que sean decidios por el hacker	Eiminando el fichero
Gusano	Por sus propios medios	Indirectos	Eliminació del fitxer

2.2_Amenazas de personas

Uno de los mayores problemas con los que se encuentran en estos momentos las empresas de todo el mundo son los ataques directos que llevan a cabo los hackers. Con la excusa de intentar «investigar sobre seguridad», intentan entrar en los ordenadores de las empresas, reventar sus contraseñas y hurgar en sus contenidos.

Los objetivos de estas intrusiones suelen ser dos: conseguir información que haya en los ordenadores o instalar programas espía. La información almacenada en un ordenador es muy valiosa, y aunque pueda parecer que en una pyme no hay grandes datos financieros, siempre hay un listado de clientes o proveedores, proyectos, estados financieros, facturación… toda esa información puede volverse muy útil para delincuentes, que pueden hacer muchas cosas con ella: venderla a la competencia, chantajear al dueño, etc.

Además, como indicábamos antes, es posible que se instalen programas espía dentro del sistema. Estos programas pueden llegar a robar contraseñas (incluso las de la conexión a los bancos), documentos o incluso servir de plataforma para lanzar ataques contra otros ordenadores.

Por otro lado, no debemos olvidar que las amenazas no siempre provienen del exterior. Dentro de las empresas están los empleados, que puede resultar una amenaza, generalmente por desconocimiento del uso de los sistemas. Los empleados insatisfechos o despechados también son peligrosos, por supuesto, pero no entrañan más riesgo para un ordenador que el que supone para un almacén físico o la cafetera.

Una persona sentada a un teclado puede, sin saberlo o sin quererlo, ser la principal vía de entrada de peligros en un ordenador. No hay que olvidar que en el fondo un ordenador no va a hacer nada por sí solo, sino que debe ser manejado por alguien, y ese alguien debe hacerlo con cuidado. Una descarga de un inocente programa o un correo electrónico abierto cuando no se debe puede resultar tan peligroso como un ataque dirigido desde el exterior.

2.3_Amenazas por datos

Aunque parezca complicado, los datos también pueden suponer un peligro. Esta amenaza se materializa generalmente en correos electrónicos, que pueden ser los correos en cadena (como los bulos que solicitan di-

nero para curar a un niño) o los envíos publicitarios no deseados, el infame spam.

Esta amenaza no entraña riesgos de destrucción de información, pero no por ello debe pensarse que es poco peligrosa. Conlleva una pérdida de tiempo muy grande para los empleados, ocupa especio de almacenamiento en los sistemas, ancho de banda de comunicación… y en muchos casos, como los «timos nigerianos» o los falsos premios de lotería, un riesgo económico para las personas.

3_¿POR DÓNDE ENTRAN LAS AMENAZAS?

Cualquier punto de entrada de ficheros o documentos externos a la empresa puede ser una vía de infección y propagación de virus a través del sistema de ficheros o correo electrónico. Este hecho además de poner en peligro la integridad de los datos de la propia compañía puede crear graves perjuicios de imagen en el caso que estos virus salgan al exterior e infecten a cualquier empresa con la que se establezca una comunicación a través de una transferencia de ficheros o correo electrónico.

3.1_Disquetes

Aunque cada vez más en desuso, las disqueteras son una de las vías de acceso de los virus al sistema con el consiguiente riesgo de propagación de dichos virus por todo el sistema de ficheros o correo electrónico.

Además del peligro de infección por ser un punto de entrada de ficheros y mensajes de correo electrónico al sistema los disquetes tienen el peligro añadido que pueden ser infectados por virus de boot (arranque). Si el usuario se deja un disquete infectado con un virus de boot en la disquetera, la próxima vez que arranque el ordenador, el sistema intentará arrancar desde el disquete, infectando inmediatamente el ordenador sin que el usuario haya realizado ninguna operación específica para ello.

3.2_Discos extraíbles, memorias USB, CD

La problemática de estos discos es similar al de las disqueteras. A través de estas unidades se pueden introducir en el parque ficheros y mensajes

de correo electrónico con el consiguiente riesgo de infección y propagación por toda la red.

3.3_Conexión de portátiles a la red

Este es uno de los puntos de mayor riesgo de infección de virus en la red debido a su mayor capacidad de conexión con el mundo exterior:

- La existencia de disqueteras en estos ordenadores.
- Su habitual conexión al exterior a través de las líneas telefónicas, redes extrañas o conexiones WiFi.
- Conexión directa a Internet independiente del resto de los sistemas de la empresa.

3.4_Sistema de mensajería

Debido a su capacidad de transmisión de documentos y ficheros con el exterior es otro punto de entrada de virus. Además el correo electrónico tiene la agravante de ser uno de los mayores medios de expansión de virus debido a su facultad de enviar un mensaje a un grupo de personas o a todo el parque a la vez. Una vez infectado un mensaje, la infección de todo el parque es cuestión de pocas horas.

3.5_Conexión a Internet

Internet es el mayor medio de transmisión de ficheros del mundo. El hecho que en Internet se encuentren colecciones de virus a disposición de cualquier persona conectada a ella permite, además de la infección accidental, la infección provocada del sistema.

4_CÓMO LUCHAR CONTRA LAS AMENAZAS

Bajo este epígrafe podría construirse un libro completo sobre seguridad informática. Nos limitaremos aquí a elaborar una lista de elementos a proteger.

Quizá la persona que lea esto descubre que se habla de una serie de protecciones que no aplican en su negocio, pero a la hora de hablar de proteger una pyme hay que cubrir numerosos aspectos, dada la diversidad de configuraciones existentes.

Cualquier protección de seguridad debe contar con unas protecciones básicas, que se encargarán de evitar intrusiones de distintos tipos:

1. Antivirus
2. Firewall
3. Detección de amenazas desconocidas
4. Auditorías periódicas

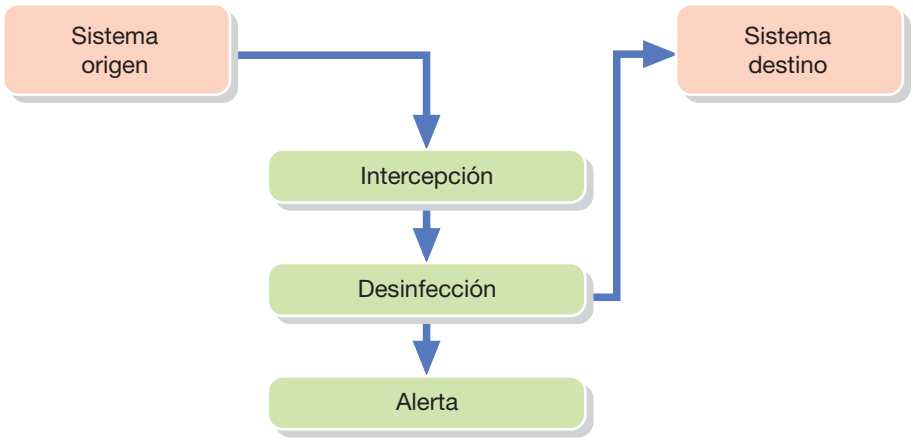
5_LOS ANTIVIRUS

Desde los primeros virus, creados como experimentos en los años 80 hasta los últimos, una de las mayores preocupaciones de cualquier usuario de ordenador ha sido la entrada de códigos malignos en su sistema.

Para evitar que los virus disfruten de nuestro ordenador solamente hay dos soluciones: una, la «burbuja»; es decir, desconectar el equipo de la red o de Internet y prescindir de cualquier lector de disquetes, CD-ROM o unidades extraíbles. Así tendremos la absoluta seguridad de que no va a entrar ningún virus. Pero tampoco entrará ningún dato que no sea por el teclado, lo que haría de nuestro ordenador una bonita máquina, pero completamente alejada de lo que es la informática: el tratamiento automático de la información. Si no hay información que entre, no se podrá tratar. Si ese es su punto de vista, le podemos recomendar un montón de espectaculares hornos microondas que le darán más servicio que un ordenador «burbuja».

La segunda solución es la instalación de un programa antivirus. Con ellos podrá tener la seguridad de que ningún código maligno entrará en nuestro sistema, pero ¿cómo lo hacen?, ¿por qué un antivirus permite que instale un juego y no permite que se copie un virus? Veamos cómo funciona.

Un programa antivirus no es más que un sistema que analiza información de muy diverso tipo y, en caso de que se encuentre infectada, procede a su desinfección. El análisis de la información se produce de muy diferentes maneras dependiendo de dónde provenga. Evidentemente no es lo mismo que un antivirus se dedique a controlar la actividad de la disquetera que la del correo electrónico o la de la red local. El principio de funcionamiento es similar, pero con matices.



[La información que está en el «Sistema origen» debe llegar al «Sistema destino». El sistema origen podría ser un disquete y el sistema destino el disco duro del ordenador, o bien el origen podría ser un servidor de Internet donde está almacenado un mensaje y el destino el ordenador personal de un usuario.

El funcionamiento del mecanismo de interceptación de la información varía en función de su implantación en sistemas operativos, en aplicaciones o bien de la necesidad de mecanismos especiales.

El mecanismo de interceptación debe ser específico para cada sistema operativo o componente sobre el que se va a implantar el antivirus. Por ejemplo, en Windows XP se utiliza un sistema, en un servidor Linux, otro, en un servidor de correo electrónico, todo depende de qué sistema sea y qué elementos se van a utilizar.

En el caso de los antivirus no diseñados directamente para sistemas operativos sino para implementarse sobre otras aplicaciones, el mecanismo de intercepción es distinto. Por ejemplo, en el caso de un antivirus para Firewalls, es el propio firewall el que facilita la información al antivirus para su análisis. En el caso de un antivirus para ficheros, hay que «robar» la información al sistema para analizarla.

En determinadas ocasiones no existe un mecanismo propio de interceptación proporcionado por el antivirus o por la aplicación. En este caso, se deben utilizar mecanismos especiales entre la aplicación y el antivirus, es decir, recursos que intercepten la información y se la faciliten al antivirus, proporcionando una integración completa para la desinfección de los virus.

Una vez analizada la información, por el método que sea, si se ha detectado cualquier peligro, se llevan a cabo dos acciones:

1. Devolver la información limpia al mecanismo de interceptación que, a su vez, la devolverá al sistema para que siga su curso hasta el destino final. Es decir, si estábamos recibiendo un correo electrónico, dejar que el correo llegue a la bandeja de entrada, o si estábamos copiando un fichero, dejar que se termine el proceso de copia.
2. Emitir una alarma a la interfaz del usuario. Esta interfaz de usuario puede ser también muy diversa. En un antivirus para una estación de trabajo puede ser un mensaje mostrado por pantalla, pero en una solución para servidores la alarma puede consistir en un mensaje de correo electrónico, un mensaje a la red interna, una entrada en un informe de actividad o una comunicación de algún tipo a la herramienta de gestión del antivirus.

Como vemos, el antivirus no hace ningún milagro extraño, ni es una pieza de software a la que debamos mirar con extrañeza. Es un aliado de nuestra seguridad, muy sencillo, pero de una elevada tecnología y precisión. Pensemos que para copiar unos cuantos megas a nuestro disco duro el antivirus debe buscar entre casi dos millones de virus sin que la marcha normal del equipo se interrumpa ni el usuario lo perciba demasiado.

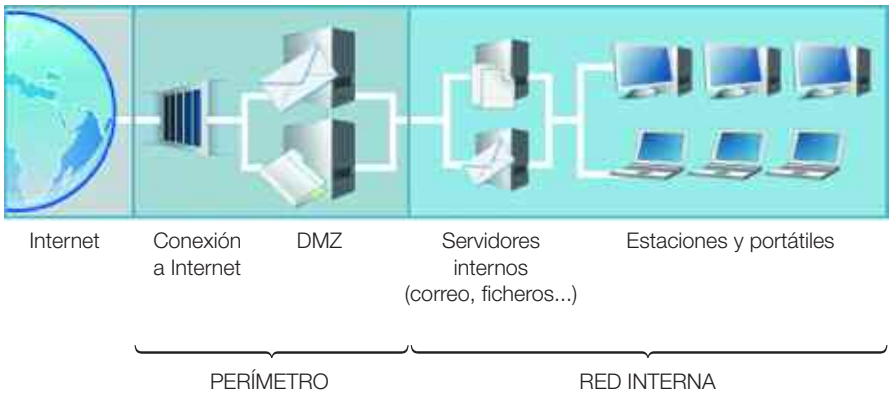
6_PROTECCIÓN EN REDES DE PYMES

La protección de una red no es una cuestión de sistemas globales. Cada punto a proteger exige a la solución de protección unas necesidades específicas a cubrir, y en ningún caso puede intentar suplantarse una protección por otra, ya que el fracaso del sistema está asegurado. Así, por ejemplo, una pasarela de correo electrónico no podrá ser protegida empleando un sistema de vigilancia de archivos, puesto que se verá abocada al fracaso.

Vamos a empezar este estudio llevando a cabo una disección de la estructura típica de una red corporativa. Como todo paradigma, su implementación distará mucho en cada caso real, pero siempre podrá extraerse de estos puntos un guión sobre el que luego adecuar la protección a cada red.

Dividiremos la red en distintos elementos a proteger de manera individual pero en sintonía con un entorno global de seguridad:

1. Puntos de conexión al exterior. Estas zonas de conexión son los «tubos» por los que se llevan a cabo las conexiones al exterior. Generalmente, con un ISP o con líneas propias, pero recibiendo o emitiendo datos a un entorno fuera de la responsabilidad de la persona encargada de la seguridad.
2. Los servidores perimétricos. El perímetro de la red está formado por los servidores que llevan a cabo las conexiones físicas con Internet, como son los firewalls o las pasarelas de correo. En ellos la protección antivirus debe extremarse, ya que un virus en ellos puede hacer que todas las comunicaciones de la empresa se vean detenidas, causando un gran daño en la continuidad del negocio.
3. Los servidores de la «zona desmilitarizada». La zona desmilitarizada o DMZ es la zona de la red informática que se encuentra abierta al público, generalmente donde se sitúan los servidores de la empresa en los que se alojan los servicios de Internet al público.
4. Los servidores internos de la empresa. En ellos se almacena toda la información básica para la continuidad del negocio, desde bases de datos a informes o la facturación. También pueden encargarse de la distribución del correo electrónico de la empresa a las estaciones de trabajo. Su protección antivirus es muy importante.
5. Los puestos de trabajo. Al ser el punto final en el que los virus se ejecutan, son uno de los puntos más importantes a proteger dentro de una empresa. Un virus propagándose por los puestos de trabajo de una empresa puede llegar a dejar paralizada la empresa en muy pocos minutos.



6.1_Puntos de conexión al exterior

Los antivirus ya no son un programa de lujo ni una extravagancia del responsable de sistemas, sino que, ante las pérdidas millonarias que han sufrido muchas empresas, todos los estamentos directivos de las corporaciones ven la protección como algo básico. Sin embargo, el concepto de protección perimetral no está tan extendido. Cuando hace un tiempo se pensaba en proteger contra virus un sistema completo, únicamente se protegía el punto de la red en el que los virus se manifestaban con toda su crudeza: las estaciones de trabajo. Protegiendo esas estaciones, la red debería quedar bien asegurada.

Pronto se vio que ese concepto de protección no era el adecuado. La proliferación de sistemas operativos fáciles de administrar y orientados a redes hizo que las redes locales empezaran a ser empleadas masivamente, y la ausencia de un sistema de seguridad adecuado en los servidores hacía inútiles los esfuerzos de la protección antivirus instalada únicamente en las máquinas de los usuarios para mantener a raya a los virus. De esa manera, aunque se evitase la presencia de códigos maliciosos en las estaciones de trabajo, siempre existía un perfecto repositorio de virus en el servidor de ficheros.

La misma evolución de las redes hacia los sistemas de trabajo en grupo provocó la aparición del correo electrónico como herramienta interna dentro de las empresas, si bien la explosión del uso de Internet en los años 90 del pasado siglo provocó un uso masivo del e-mail. Por tanto, surgió la necesidad de proteger contra los virus el punto de entrada de los mensajes, instalándose los antivirus en los servidores de correo electrónico de la empresa.

El aumento de las conexiones a Internet y la necesidad de un mayor nivel de seguridad en las comunicaciones de la empresa propiciaron el uso de servidores proxy y firewalls. Siendo estos sistemas una gran puerta de entrada de virus (de hecho su nombre en inglés es «gateway», pasarela), la necesidad de instalar allí un antivirus es evidente. Así, pasaron a engrosar la lista de sistemas protegidos contra virus en una red corporativa.

Pero llegados a este punto, en el que las redes locales no son más que una pequeña prolongación de Internet dentro de las empresas, la protección debería ir un paso más allá. Si el firewall o la pasarela de correo se

consideran ahora mismo el perímetro de la empresa, ¿por qué no llevar la protección al perímetro exterior de la red?

El perímetro exterior es un punto muy pequeño de la red. Es vital para la comunicación y la continuidad del negocio, pero físicamente pasa desapercibido ante unos ojos no entendidos. Se trata del punto en el que se conecta la red a Internet, la línea de comunicación o, como se le conoce en el argot técnico, el «tubo» por el que entra toda la información.

Pero en ese «tubo» tenemos dos puntos distintos, que son los dos extremos del cable de comunicación. Uno de ellos está en la empresa, el punto real de conexión al proveedor. Si en ese punto se coloca un sistema de protección antivirus, la estructura interna de la protección (firewalls, proxy, estaciones de trabajo, etc.) se verá descargada de un trabajo muy importante y la mayor parte del tiempo de proceso podrá emplearse en tareas internas de la empresa y, en definitiva, en contribuir a la continuidad del negocio.

Por otro lado, y justo en el otro extremo del «tubo», se encuentra nuestro proveedor de servicios de Internet. En él confiamos para que el ancho de banda no decaiga, para que nuestras comunicaciones sean fiables y toda la información que entre y salga de la empresa lo haga rápida y fiablemente. Pero aunque exigimos (y el proveedor nos ofrece) una serie de características, normalmente no valoramos si nos brinda la información sin peligros víricos. En ese otro punto es donde se debe exigir al proveedor la instalación de un sistema de protección antivirus y en caso de que no lo ofrezca, tenerlo en las instalaciones corporativas.

El principal problema reside en la necesidad de que el sistema instalado para la protección antivirus en el perímetro exterior de la empresa sea sencillo de gestionar y tenga capacidad adecuada para analizar todo el tráfico de la red sin merma en los servicios de comunicaciones que se brindan a los usuarios de la red.

Las soluciones para la protección avanzada del perímetro exterior de la red están basadas en muchos casos en sistemas software que se instalan sobre una máquina propia de la compañía. Esta solución proporciona gran tranquilidad a la empresa ya que se posee un buen control sobre el software y el hardware.

El problema es que, con mucha frecuencia, las máquinas en las que se instalan los sistemas de protección antivirus del perímetro suelen estar

relativamente obsoletas y, aunque tanto el procesador como la memoria o el disco duro sean suficientes para una tarea específica, han dejado de ser válidos para soportar toda la distribución de correo electrónico de la empresa o funcionar como sistema de almacenamiento de ficheros.

Cada vez se tiende más a utilizar dispositivos hardware diseñados específicamente para una tarea concreta, como pueden ser los dispositivos «Network Attached Storage» (NAS) o los firewall basados en hardware. Sin embargo, la fiabilidad de los elementos específicos se ha visto demostrada como mucho más alta que las de los sistemas generalistas (o máquinas con un sistema operativo que pueden albergar varios servicios) dedicados a una tarea en concreto.

Además, las soluciones específicas para tareas específicas brindan a las empresas la posibilidad de crecer para acomodarse a los requerimientos de cada momento. Con la filosofía de la ampliación siempre presente, los diseñadores de estos equipos les han provisto, por ejemplo, de sistemas de balanceo de carga para evitar tener que llevar a cabo tareas complejas de configuración y puesta a punto. En el caso de los sistemas generalistas, el pensar en una ampliación añadiendo un determinado servicio al sistema, supone normalmente una parada de los equipos que, en muchos casos, puede suponer pérdidas económicas (bien por errores de configuración, pérdidas de datos o simplemente por lucro cesante) que no deben ser permitidos.

Aunque a nadie le guste, el software del que disponen las empresas sigue teniendo fallos y vulnerabilidades, en cuyas soluciones los desarrolladores ponen su máximo empeño. Pero la corrección de un error, por pequeño que sea, puede suponer una parada del sistema y un cierto tiempo de intervención del responsable. Y en muchos casos, la instalación del «parche» puede hacer que las máquinas se vuelvan inestables. Además, con demasiada frecuencia se instalan actualizaciones de sistemas que no son necesarias por no tener en producción una determinada tarea.

En un sistema dedicado, las tareas de mantenimiento son mínimas. Al tener su objetivo tan claramente delimitado, los posibles problemas que puedan afectar al sistema están perfectamente contemplados y previstos. El caso paradigmático de esta situación es un antivirus que, para su correcto funcionamiento, necesita ser actualizado, al menos, una vez al día. Si cualquier componente del sistema no está previsto para que este evento se produzca con la frecuencia necesaria, nos encontramos con un serio problema.

Además, que el mantenimiento del sistema sea absolutamente desatendido y automático debe ser una tarea tan primordial para estos sistemas como aquella para la que fueron diseñados. Si el firewall necesita parar durante unos minutos al día estaremos, o bien eliminando la seguridad de la red, o cortando un servicio de comunicaciones en la empresa. Sin embargo, si su mantenimiento se ha contemplado como un proceso más y ha sido preparado para que no se interrumpa el servicio ni se requiera intervención externa alguna, podremos considerar que ese dispositivo está bien diseñado.

Cada vez que se habla del perímetro de una empresa, siempre tiende a pensarse en grandes cuartos llenos de servidores de comunicación, extraños cables que salen de armarios llenos de servidores y delicados conductos de fibra óptica. Efectivamente, dentro de esa estructura está el perímetro informático de una gran empresa, pero todo sistema conectado a otro (Internet o simplemente a otra red, sea pública o no) tiene un punto en el que se produce esa conexión y un ordenador que la controla.

La conexión puede ser de fibra óptica con un ancho de banda mareante, o una simple línea ADSL con al ancho de banda correspondiente a la oferta de turno del proveedor, pero en cualquier caso el sistema que efectúa la conexión está en el perímetro de la red. Por pequeña que sea la empresa, mientras tenga una conexión tendrá un perímetro que proteger.

Precisamente por la creencia de que la protección perimetral es un tema de grandes sistemas, las medianas empresas no se protegen como deberían. Evidentemente en muchos casos estas empresas no tienen una infraestructura de red suficiente para que les compense tener una persona dedicada al mantenimiento de equipos, y mucho menos a la seguridad.

Para solventar este problema, las medianas empresas -y cada vez más las pequeñas- recurren a otras empresas especializadas en informática que se encargan de todo el mantenimiento de los equipos, la red, las comunicaciones... Gracias a ellos sus sistemas informáticos están permanentemente atendidos y en perfecto orden de marcha.

A la hora de establecer una protección antivirus, y más en el perímetro, la accesibilidad al sistema antivirus debe ser cómoda para el administrador, tanto si lo hace desde dentro de la red como si es desde fuera. Evidentemente, si se sigue esta premisa la capacidad de reacción ante cualquier

problema se incrementa sobremanera al poder resolver una incidencia en remoto, o simplemente recoger los informes de actividad del antivirus.

Una protección perimetral antivirus deberá tener una serie de características básicas que la hagan realmente eficaz. Estas deberán ser las siguientes:

- **Solución específica hardware-software.** Tanto el software como el hardware deberán estar orientados única y específicamente a la búsqueda y eliminación de virus, sin que los recursos del sistema ni los elementos hardware estén ocupados en tareas distintas a la defensa antivirus.
- **Alto rendimiento de la protección antivirus.** El sistema a instalar debe ofrecer un extraordinario rendimiento y capacidad de análisis. Además, su funcionamiento debe ser completamente transparente para la red corporativa.
- **Alta capacidad de ampliación y balanceo de carga.** Un sistema de protección antivirus debe ser completamente ampliable para poder adaptarse a las necesidades de cualquier tamaño de empresa, además de ajustar su capacidad de análisis a las comunicaciones de la red.
- **Gran sencillez de instalación y configuración.** La instalación de un sistema antivirus no puede ser una tarea complicada que haga que los administradores de red utilicen tiempo adicional en ellas. Tanto la implantación como su configuración para la puesta en marcha deben ser sencillas e inmediatas.
- **Protección para los principales protocolos de comunicación.** Debe cubrir todas las necesidades de protección antivirus de la red frente a las amenazas de Internet de una manera sencilla y eficaz.
- **Sistemas de inspección profunda de paquetes.** Con ellos, se podrán detectar paquetes malformados y detectar, en tiempo real, posibles ataques que luego se manifestarán en otros servidores o estaciones de trabajo.
- **Filtrado de contenidos, para impedir que los virus desconocidos y los gusanos informáticos entren en la empresa.** Deberá evitar el excesivo consumo de recursos y ancho de banda de la red, deteniendo los contenidos potencialmente peligrosos incluso antes de que entren en la red interna.

- **Administración remota.** La gestión de la protección debe hacerse de forma remota y segura a través de interfaces amigables, aportando al administrador flexibilidad en el acceso desde cualquier ordenador. Asimismo, debe poder accederse a ella no solamente desde el interior de la red, sino que, con los debidos sistemas de seguridad, debe ser accesible también desde el exterior para llevar a cabo tareas por personal ajeno a la empresa.
- **Actualizaciones diarias y automáticas.** El sistema de actualizaciones contra los nuevos virus debe estar configurado por defecto para que se realice de manera automática y prácticamente continua. Así, dispondrá siempre de la última actualización disponible, permaneciendo totalmente actualizado contra cualquier nuevo virus que pueda aparecer.
- **Informes detallados y alertas personalizables.** Para que los administradores sepan qué está pasando con la protección antivirus, deberán tener a su disposición informes de la detección de virus y del filtrado de contenidos realizados, al igual que alertas y notificaciones personalizables sobre la actividad de la protección antivirus.

6.2_Servidores perimétricos

La misión de un firewall es restringir el acceso a una parte de la red. Se puede utilizar tanto para evitar que alguien del exterior de la red entre a servidores internos como para que los usuarios internos acceda a determinados recursos exteriores. Generalmente la instalación de un firewall se realiza en el punto en el que la red empresarial se conecta al exterior, ya que por allí deben pasar obligatoriamente todas las comunicaciones.

Dado que todo el tráfico que entra desde Internet o sale desde la red interna lo hace a través del firewall, éste puede examinarlo y posee la potestad de decidir si es aceptable o no y si lo hará llegar a su destinatario. Ahora bien, es fundamental definir correctamente lo que significa «aceptable». Para ello se confecciona una política de seguridad (las reglas del firewall), en la que se establece claramente qué tipo de tráfico está permitido, entre qué origen y qué destino, qué servicios se habilitan, qué contenidos se admiten, etc. Dependiendo de cada caso concreto, existirán políticas altamente restrictivas -en las que prácticamente nada está permitido- y otras muy permisivas, en las que no se habilitan apenas prohibiciones. La clave reside en alcanzar un compromiso entre las necesidades de seguridad y la comodidad.

6.3_Servidores de correo electrónico

Cerca del 90% de los virus informáticos que entran en las empresas lo hacen a través del correo electrónico. Esta elevada cifra se debe fundamentalmente al elevado uso que se produce del mismo por parte del usuario, que no solamente intercambia mensajes de texto para fines empresariales, sino que en un elevado tanto por ciento de los mensajes se incluyen ficheros adjuntos, tales como documentos, presentaciones, etc.

En la práctica los usuarios del correo intercambian no sólo mensajes con fines laborales, sino con otras personas, en muchos casos ajenas a la empresa, a las que se les mandas bromas, chistes, ejecutables humorísticos, etc.

Recibir un e-mail con un determinado mensaje extraño, o con un ejecutable que no tiene nada que ver con el trabajo se convierte en tan habitual como los mensajes internos de la empresa.

Si dejamos aparte las consideraciones sobre la legalidad o ilegalidad, tanto de manejar este tipo de mensajes como su control por parte de la empresa, se ve absolutamente necesario evitar que en los servidores de correo se almacenen ficheros que puedan resultar peligrosos para la seguridad de la compañía.

Cualquier código ejecutable que penetre en la empresa puede ser susceptible de contener virus. No debemos esperar que porque no se haya desarrollado todavía un determinado tipo de virus en un determinado sistema no haya peligro para la red. Desde los obvios, como los ficheros EXE o COM, hasta los más insólitos, como algunas versiones de Shockwave Flash, todos ellos pueden contener código maligno en mayor o menor grado. Por tanto, el filtrado de los elementos adjuntos al correo electrónico debe estar activo en todo momento.

El correo web es la solución más útil para las personas que necesitan consultar sus mensajes desde cualquier parte del mundo. Mientras que la configuración de un lector de correo POP a veces es complicada, el acceso a una página web es básico en cualquier ordenador conectado a Internet.

Los correos electrónicos que se leen en páginas web conllevan un peligro no siempre apreciado a simple vista. Muchos firewalls analizan SMTP y POP3 para evitar los virus por correo electrónico, pero en el caso de los

correos web la información viaja por HTML, por lo que el análisis puede no llevarse a cabo.

El análisis de código HTML debe producirse con los mismos niveles de seguridad que emplean los administradores con el tráfico SMTP y POP3. Un virus que se propague por correo electrónico también va a difundirse a través de un correo web, además con consecuencias negativas para el propietario de la máquina, ya que las direcciones de correo electrónico que un gusano emplearía para difundirse serían las del ordenador en el cual se consulta el correo, no las de la dirección de correo web.

6.4_Filtrado de contenidos

El filtrado de contenido debe funcionar a dos niveles distintos: en los servidores de correo corporativo y en las pasarelas que proporcionen salida de información a Internet. Usar únicamente filtrado de contenidos en uno de los puntos proporcionaría una protección inadecuada por las siguientes razones:

- Si se emplea únicamente en los servidores internos de correo, cualquier utilización del correo electrónico con herramientas distintas a las corporativas produciría un agujero en el filtrado. Baste pensar que en cualquier plataforma Windows entre Windows 98 y Vista, aparece Outlook Express como lector de correo electrónico por defecto. Y leer el correo electrónico sin necesidad de pasar por el servidor corporativo, por ejemplo Exchange Server, es muy fácil, pero siempre deberá atravesar el firewall.
- Si únicamente se dispone de filtrado en el servidor de correo externo, los correo electrónicos que no pasen por el firewall se verán libres del control. Es decir, que un virus, un «hoax», un mensaje inapropiado o cualquier mensaje que la empresa no considere necesario no saldrá de la empresa, pero su circulación será inevitable dentro de la misma, con lo que el problema, si bien no sale al exterior, estará en la red interna sin control.

El filtrado debe ser un elemento integrado con el resto de sistemas que estén manejando el correo electrónico. Colocar dos sistemas distintos de análisis, como puede ser un antivirus y un sistema de filtrado, o un mecanismo de firma corporativa y un filtrado, producirán un retraso inaceptable en la entrega y en el envío del correo electrónico, que si bien

puede ser muy poco significativo dada la filosofía de no-instantaneidad del correo electrónico, puede producir saturaciones puntuales y caídas en la efectividad del servicio de correo.

El filtrado debe poder hacerse en función de dos parámetros:

- El asunto del mensaje de correo electrónico. Permitiría eliminar drásticamente el «spam» y determinados mensajes publicitarios o los «hoaxes».
- Los ficheros que vayan adjuntos, lo que posibilita limitar ficheros bien por nombre, por extensión o por ambos.

Mediante el filtro, el administrador del sistema podrá actuar sobre ficheros o mensajes perniciosos, sin tener que detener el servidor de correo ni el firewall y llevar un exhaustivo control de la mensajería entrante y saliente sin interferir en ella.

6.5_Los servidores de la «zona desmilitarizada»

La «Zona desmilitarizada», también conocida por sus siglas en inglés, DMZ o «de-militarized zone» (DMZ), es un área de la red (una subred) que está situada entre la red interna de una empresa y una red externa, generalmente Internet.

En esta zona de la red están permitidas las conexiones desde dentro y fuera de la red a la DMZ, mientras que las conexiones desde la DMZ solamente se permiten al exterior: los servidores en la DMZ no deben conectar con la red interna.

Así se permite a los servidores de la DMZ proporcionar servicios tanto a la red interna como a clientes externos, protegiendo la red interna de posibles intrusos. Para alguien que desde fuera se conecte a la DMZ, se encuentra que es un callejón sin salida y no puede pasar más allá.

Los servidores de la DMZ suelen ser únicamente servidores de archivos, para servicios web, consulta de bases de datos, etc. Por lo tanto, su protección contra malware pasa por un escáner de ficheros residente, de manera que cualquier cambio en un fichero o la llegada de un fichero nuevo sea inmediatamente analizado por el sistema de protección.

Hay un elemento importante en esta protección que debe evaluarse con sumo cuidado. En un sistema web de una DMZ habrá, en prácticamente todas las ocasiones, una base de datos, gestionada por algún

sistema. La protección de esta base de datos es importante, pero debe tenerse en cuenta que el análisis de los ficheros que pasan a engrosar la base de datos debe hacerse antes de que se añadan a la base, nunca hacerse el análisis de la base de datos globalmente. De hacerlo así, se producirá una ralentización general del sistema, ya que las bases de datos tienen generalmente mucho tamaño y mucho contenido a analizar, además de estar siendo modificadas muy frecuentemente.

En estos casos lo mejor es instalar un sistema de análisis de tráfico, en lugar de una protección basada en host, es decir, instalada directamente en el ordenador.

6.6_Los servidores internos de la empresa

El concepto de servidor interno de una red abarca a numerosos equipos que se pueden encargar de las más diversas tareas. Desde la más extendida como servidor de archivos hasta los equipos que se encargan de distribuir el correo electrónico en distintos departamentos de la empresa, servidores con equipos de cinta para copias de seguridad, servidores de pruebas, de CD ROM...

Estos servidores internos suelen ser en muchos casos los grandes olvidados de la seguridad empresarial. La mayor parte de los esfuerzos de protección se vuelcan en los equipos perimetrales, como firewalls, y en las estaciones de trabajo al estar expuestas a las acciones directas de usuarios maliciosos o simplemente inexpertos.

Su protección antivirus es tan importante como la del resto de las máquinas, ya que aunque el funcionamiento de la empresa no dependa directamente de ellos, su infección por un virus puede acarrear tantos problemas como la infección de un firewall. En este documento nos ocuparemos de ver cómo implementar un antivirus en estas máquinas, sin olvidar que las soluciones antivirus son el final de un proceso que debe comenzar con una la configuración preventiva del sistema.

El primer paso para la protección efectiva de un servidor es, obviamente, la instalación del antivirus en el sistema. Pero debe recordarse que en función de la tarea a la que se destine ese sistema deberá tener un antivirus específico.

Como norma general, cualquier ordenador deberá protegerse empezando por el sistema operativo en el que funciona independientemente de la

tarea a la que se destine después esa máquina. Es decir, si hemos instalado un sistema con, por ejemplo, Windows, deberá instalarse allí un antivirus específico para Windows. O si es Linux, un antivirus diseñado para Linux.

Posteriormente, en caso de que se instale algún servicio más sobre el sistema (correo electrónico, proxy, etc.) habrá que instalar un sistema antivirus diseñado específicamente para ese servicio que funciona sobre el sistema operativo.

Cualquier sistema operativo para servidores de red ofrece como característica básica y fundamental la posibilidad de convertir el servidor en un servidor de ficheros. Así, los usuarios de la red pueden compartir programas, documentos... y virus. La instalación de un antivirus en los servidores de ficheros se vuelve básica.

Para hacerlo, se deben tener en cuenta los siguientes puntos:

- La disponibilidad de los servicios no debe verse interrumpida por la instalación del antivirus.
- Los usuarios no deben notar que caiga el rendimiento de la máquina tras la instalación del antivirus.
- La actualización del antivirus debe ser automática.
- El antivirus debe proporcionar alertas al administrador de la red, no a los usuarios.
- La instalación debe realizarse de manera remota y centralizada, así como su gestión, tanto en redes locales como en WAN.

7_HEURÍSTICO VS. INTELIGENTE

Las técnicas de detección de virus están influidas por palabras que nos sorprenderían por su antigüedad. Aunque parezca increíble, los dos términos que describen los sistemas básicos de detección de virus -heurístico y algorítmico- tienen más de mil años de edad.

Algoritmo proviene del nombre de un matemático árabe: Muhammad ibn Musa abu Djafar Al-Khorezmi. Más conocido por «Al-Khorezmi», nació alrededor del 780 DC en Khorezm, el actual Uzbekistán. Él fue el primero que diseñó algoritmos pensando en su eficiencia para el cálculo de raíces de ecuaciones.

El método algorítmico de detección de virus, comúnmente llamado de búsqueda de cadenas de virus, consiste en localizar una determinada cadena de caracteres en un fichero. Si esta encontrada, el fichero está infectado por un virus. Es el sistema más efectivo para encontrar virus con gran precisión, ya que (siguiendo la definición de algoritmo) lleva a cabo un «conjunto ordenado y finito de operaciones» para la detección.

El otro sistema de detección de virus es el heurístico. En la práctica, el sistema de detección heurístico de un antivirus es capaz de hallar virus completamente desconocidos. Como si fuera Sherlock Holmes, el antivirus investiga el comportamiento del código ejecutable que haya en los archivos. En caso de detectar alguna posible amenaza, avisará al usuario del ordenador para que tome las medidas oportunas.

Aunque la base de este sistema puede parecer sólida, encuentra numerosos inconvenientes a la hora de ser implementada. La peligrosidad de un fichero no debe ser evaluada basándose única y exclusivamente en una instrucción. A pesar de que en los mejores sistemas heurísticos se llevan a cabo varias comprobaciones, el sistema produce demasiados falsos positivos (ficheros detectados como sospechosos cuando no lo son) y falsos negativos (ausencia de alarma cuando el material analizado es realmente peligroso).

Para poder llevar a cabo una detección inteligente debe irse más allá del simple análisis de ficheros que entran o salen en un sistema, deben controlarse los programas en ejecución en cada momento en el sistema. Así, cualquier instrucción o tarea sospechosa de constituir un peligro será monitorizada y vigilada de manera especial. Y digo vigilada, ya que antes de alertar al usuario debe comprobarse exactamente qué está haciendo. Una acción no es peligrosa por sí sola (que un sistema heurístico sí clasificaría como peligrosa), sino que hay una serie de tareas paralelas o de situaciones en el entorno que marcan la peligrosidad. Esa es la tarea que el antivirus inteligente debe llevar a cabo: el análisis y la comprensión de qué está pasando.

Podemos ver un ejemplo muy claro con la orden «FORMAT». Como todo el mundo sabe, esta instrucción sirve para formatear un disco, eliminando los contenidos existentes y dejándolo vacío para un nuevo uso. Aplicada a un disco duro puede ser realmente peligrosa, dejaría a un ordenador sin ningún contenido.

Esa instrucción utilizada en un ordenador puede ser empleada de varias maneras. Por ejemplo, un programa que intente formatear el disco duro principal, sin mostrar ningún mensaje, sin esperar ninguna confirmación por parte del usuario y activándose al llegar una determinada fecha tiene una inmensa probabilidad de que sea malicioso. Sin embargo, la misma instrucción desde una ventana de comandos abierta mediante movimientos de ratón aplicada a un disquete tiene una apariencia completamente distinta.

Un sistema de seguridad que realmente quiera proteger los equipos en los que esté instalado necesita una serie de detectores de peligrosidad que puedan alertar ante determinadas situaciones que, combinadas, supongan un peligro. No estoy hablando de una especie de lista de situaciones, sino de un sistema que realmente pueda entender y comprender qué está pasando dentro del sistema. No cabe duda de que son muchos los elementos a analizar y evaluar, pero haciendo un repaso a las amenazas más importantes de los últimos tiempos podemos inferir la problemática asociada a los próximos códigos maliciosos.

8_NANOTECNOLOGÍAS Y SOFTWARE MALICIOSO

El que se considera primer ordenador electrónico programable es el ENIAC, construido como sistema de propósito general (es decir, capaz de llevar a cabo diferentes tareas en función del programa que se le suministrara). Los operarios del sistema tenían que tener muchísimo cuidado con los programas que elaboraban, ya que un error suponía un montón de tiempo de revisión de las tarjetas perforadas que le suministraban información. Y los programas debían ser muy pequeños, ya que su memoria era pequeña, disponía de 17.468 tubos de vacío capaces de almacenar números: cada 36 tubos almacenaban un número.

¿Cómo debían sentirse las personas que manejaban los datos de ese sistema? Supongo que como un biólogo pegado al microscopio, mirando cada dato, cada número, cada instrucción, para que cupiera en la exigua memoria del sistema.

Rápidamente empezaron a crecer en capacidad y velocidad los ordenadores, y el primer PC (el de IBM, el modelo 5150) ya era capaz de almacenar 16.384 números en su memoria basada en transistores. La pequeña (por aquel entonces) empresa Microsoft había desarrollado un

intérprete del lenguaje Basic que únicamente ocupaba cuatro kilobytes, y estaba incluido en la memoria ROM de ese micro ordenador. Visto ahora parece casi increíble. Que un intérprete de un lenguaje de programación sea capaz de «caber» en tan poco sitio suena a leyenda urbana.

El progreso en la informática ha facilitado que cada vez se puedan producir microprocesadores más rápidos y dispositivos de almacenamiento más fiables y todo ello más barato. ¿Quién podría imaginar que un sistema informático como el actual en 1981, cuando se presentó el IBM PC? Un microprocesador con una frecuencia de reloj que se mide en Gigahertzios, almacenamiento en disco y en memoria medido en Gigabytes, y todo ello por menos de la cuarta parte de lo que valía en su momento.

Pero sin embargo, los usuarios ¿qué han ganado con todo esto? ¿Tarda menos en hacerse una hoja de cálculo con cualquier sistema actual que hace unos años con los sistemas preparados para trabajar en pantallas de texto de fósforo verde? No mucho menos. Se hacen más bonitas, con más tipos de letra, con más efectos… pero no son mucho más efectivas. La inmensa mayoría de los usuarios desconocen el 80% de las funciones de su procesador de textos, lo que le sirve a los «expertos» de oficina a aparecer como héroes cuando enseñan cómo poner una palabra en negrita sin necesidad de separarse del teclado y usar el ratón.

El software ha ido creciendo y volviéndose cada vez más complejo ya que los sistemas lo permitían. Y ese crecimiento supone consumo de recursos: memoria, disco, procesador, tarjeta gráfica, etc. Recuerdo el paso del famoso dBase III, que dejó de ocupar un par de disquetes de 5 pulgadas y cuarto al dBase IV, que se distribuía en ¡once disquetes! Muchos se llevaron las manos a la cabeza por ese dispendio en disquetes y en espacio. Cuando al final, el uso que se le daba a ese programa era, en muchos casos, únicamente dar de alta y consultar una base de datos sencillita. ¿Cuántos usuarios llegaron a emplear el sistema de consultas SQL embebido en dBase IV?

Por no hablar de lo sistemas operativos. MS-DOS 3.3, por ejemplo, ocupaba dos disquetes de 360 Kb, MS-DOS 6, 4 disquetes de 1,44 Mb (16 veces más), Windows 95 en 13 disquetes con un formato especial que conseguía algo más de espacio, y ya dio el salto al CD ROM para instalarse. Windows Vista se distribuye en DVD, un soporte que es capaz de almacenar 4,7 Gb, es decir, más de 13.000 discos como los de la distribución de MS-DOS 3.3.

Este crecimiento ¿en qué ha repercutido? En muchos gadgets, en mucho interfaz gráfico tridimensional, en imágenes foto realistas, pero a costa de consumir recursos a mansalva.

¿Pensamos en el malware? ¿Cuánto ocupaba el Viernes 13? Utilizaba únicamente 2 Kb de memoria, y los ficheros infectados crecían en 1.813 bytes. ¿Y el gusano Brontok.FT? Más que un gusano parece una anaconda, o una serpiente pitón. ¡Ocupa 12 megabytes!

Todo crece: los discos, las memorias, las funciones del sistema operativo… ¿No es posible hacer que las aplicaciones en lugar de crecer vayan a menos? ¡Si en un reloj digital hay más capacidad de procesamiento de información que en el Apolo XI y llegó a la luna!

Pues sí, es posible. En la mecánica se está empezando a investigar en el campo de las nanotecnologías, de manera que se están construyendo máquinas a escala atómica. Por ahora son experimentos, engranajes en los que los piñones no son más que átomos o tubos por los que únicamente puede pasar una molécula. En la informática, están empezando a despuntar sistemas nanotecnológicos. Programas que, a pesar de la tendencia actual a utilizar más recursos, más memoria y más funciones, son extremadamente ligeros y rápidos.

Los nanoprogramas pueden estar diseñados para funciones muy concretas, como puede ser mostrar un pequeño reloj en pantalla, o un juego sencillo pero adictivo. O incluso funciones complejas, como la aplicación «nanoscan» de Panda Security.

Nanoscan es un sistema de búsqueda de malware activo en un sistema que es capaz de encontrar cientos de miles de programas malignos sin necesidad de ocupar megas o gigas en el sistema. Gracias a un sistema de desarrollo tremendamente cuidado y teniendo como objetivo el tamaño mínimo con las máximas funciones, se ha conseguido, por fin, hacer olvidar al mercado la tendencia a engordar el software.

¿Y cómo es posible? Sencillamente, olvidándonos de que un sistema va a poder ofrecernos más recursos de manera ilimitada. Las aplicaciones clásicas han sido desarrolladas pensando en que van a ser instaladas en un sistema lleno de API distintos, muy útiles y llenos de funciones, pero que deben ser cargados en memoria para usarlos. Y cada aplicación hace lo mismo, por lo que el consumo de recursos crece de manera desorbitada.

Si se desarrolla una aplicación prácticamente «auto contenida», sin optar por el fatware; y con un I+D realmente investigador y desarrollador, se pueden conseguir resultados impresionantes en la industria del software.

Estamos a las puertas de una nueva era, la del nanosoftware. Quizá en poco tiempo volvamos a tener que recuperar los disquetes de 3,5 pulgadas para instalar un procesador de texto. ¿Por qué no? Sólo es cuestión de tomarse el desarrollo de software como una ciencia, y no solo como una colección de archivos entrelazados comerecursos.

9_LA NUEVA DINÁMICA DEL MALWARE

La dinámica del malware ha cambiado. Dicho cambio ha venido provocado por un cambio en la mentalidad de los autores de malware, ya que antes les movía una motivación de buscar la fama («Ser el número 1») y ahora les mueve una motivación económica.

Hasta el año 2004, los autores se movían buscando la fama. Básicamente, buscaban realizar hazañas de las que pudieran hacer gala con sus amigos. Esto hacía que las epidemias fueran masivas y cada vez se propagaran más rápido. En los años 90, los virus eran locales, y se propagaban a través de disquetes. Por lo tanto, la distribución de los códigos maliciosos era muy lenta y tardaban incluso meses en propagarse.

Con la expansión de Internet, la propagación cada vez era más rápida. Gusanos como «I Love You», «Sircam», etc., fueron capaces de distribuirse en días, ya que eran tecnológicamente más avanzados y aprovechaban la circunstancia de la conectividad mundial para conseguir llegar a millones de usuarios en menos tiempo.

En los años 2000, los tiempos de distribución eran cada vez menores, incluso minutos o segundos. Por ejemplo, «SQLSlammer» fue capaz de infectar millones de servidores en sólo 15 minutos. Se comienza a hablar de amenazas «Flash», aquellas capaces de infectar en segundos.

E incluso se puso de moda los ataques «Zero days» o «Zero hours», que son aquellas capaces de aprovechar y explotar vulnerabilidades antes de que los fabricantes descubran dichos agujeros de seguridad.

Ahora, las epidemias son cada vez menos masivas, menos visibles. Desde el año 2005 apenas se han producido alertas por virus, y las alertas

han sido de muy bajo nivel. ¿Qué está pasando, nos preguntamos todos?

Lo que está pasando es que la motivación de los autores de malware está cambiando. Ahora no buscan la fama: ahora buscan dinero. Es decir, existen varias organizaciones criminales –y también empresas interesadas en conseguir secretos de sus competidores– que están financiando a los hackers, y esto provoca que éstos se profesionalicen. «Cuando mejor sepa hacer mi trabajo, más me pagarán».

Evidentemente, para hacer dinero ilegalmente es mucho mejor ser discreto y no armar ruido, por lo tanto, los autores de malware no están interesados en crear epidemias masivas y visibles. Los nuevos ejemplares de malware se hacen más ocultos, más silenciosos... Por eso, ahora las epidemias masivas han cambiado y ahora hablamos de epidemias silenciosas. No porque sean menos masivas, sino porque son menos evidentes, no salen a la luz.

El hecho de que los hackers estén financiados, hace que éstos se profesionalicen. Es decir, el malware es cada vez más sofisticado, diseñado especialmente para no ser detectado. Por lo tanto, este nuevo malware es mucho más difícil de combatir. Utilizan complejas y astutas técnicas de ocultamiento, ya que sus autores pretenden que dicho malware no sea detectado durante mucho tiempo.

Las oportunidades de negocio que ofrece la Red son cada vez mayores para individuos y empresas... pero también para los malos, que encuentran en Internet un ideal caldo de cultivo para llevar a cabo sus acciones maliciosas.

¿Y cómo consiguen dinero? Aunque hay más, pongamos dos ejemplos. El primero, es el del Botnet. Bot viene de la contracción de «robot» e identifica a un tipo de malware que permite, sin que el usuario lo sepa, coger el control del PC y esperar órdenes de un servidor. Los ordenadores que tienen este tipo de malware se dice que son PC zombis o que están secuestrados, ya que chequean de forma regular si hay trabajos que tengan que hacer. Dicho trabajos son diferentes: o lanzar spam, o lanzar un ataque de denegación de servicio DDoS, lanzar spyware... o lanzar más bots para conseguir más PC zombis.

Net significa red. Es decir, que cuando hay muchos PC zombis o secuestrados que chequean regularmente contra un mismo servidor decimos que es una Red de Bots, que está esperando instrucciones. ¿Y qué or-

denes les da? Pues depende de los que la mafia de la web, los comerciantes o afiliados le contraten. Por lo tanto, este pastor tiene unos ingresos: la contratación de sus redes de PC secuestrados.

Otro de los modelos de negocio que se dio a conocer con un caso en Israel en mayo de 2005 es el de los ataques dirigidos. Este tipo de ataques son aquéllos diseñados específicamente para llegar al ordenador de «fulanito de tal» de la empresa «tal». El hacker se informa, se documenta, se entera de cuáles son las responsabilidades de una determinada persona, gustos o preferencias, y elabora un malware diseñado no sólo para la empresa, sino que además lo hace llegar de forma personalizada.

O llegará un correo electrónico personalizado, incluso con referencias de un tercero, y ofrecerá un link al que se pueda entrar para conocer la empresa. Cuando se pincha el link, se llega a una web totalmente lícita, seria y comercial, pero sin saberlo, un troyano se estará descargando e instalando en el PC.

Estos ataques basados en modelos de negocio no son tan raros como parece. Las empresas sufren numerosos ataques, y los que están basados en códigos maliciosos (entre loo que están estos nuevos códigos con motivación económica) son los más importantes para el 82% de las empresas.

Y si ya el 12% de las empresas encuestadas valoraron las pérdidas por los ataques hasta en 100.000 dólares, ¿cuánto pueden ser las pérdidas por los códigos que llegan dirigidos a una persona? Imposible saberlo, el 62% de las empresas encuestadas no supieron cuantificar las pérdidas económicas debidas a ataques electrónicos.

Estos ataques tienen un claro vector de introducción en las empresas: el correo electrónico. Es el medio de comunicación más empleado actualmente, con la desventaja de que es fácilmente accesible y manipulable. El protocolo utilizado para el correo electrónico (SMTP) es muy simple y puede ser emulado por cualquier internauta con un mínimo de conocimientos.

Además, el servidor de correo tiene una gran cantidad de información que permite a los atacantes dirigir un ataque de manera muy efectiva: en el servidor puede conocerse la estructura organizativa de la empresa, funciones clave, etc.

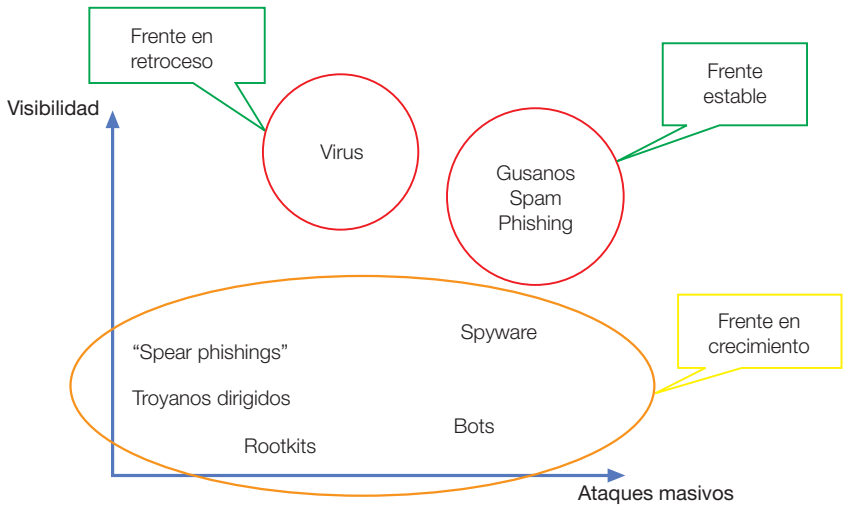
La solución puede parecer sencilla, pero en cada capa del sistema informático empresarial podemos encontrarnos con problemas de solución compleja:

- Seguridad en el PC: No ofrece protección contra ataques de denegación de servicio, los criterios de filtrado de SPAM quedan en manos del usuario, y puede sobrecargar la red.
- Seguridad en el servidor correo: puede producir una sobrecarga de los elementos de la red hasta el servidor de correo, y se añade un proceso más al servidor de correo.
- Seguridad en gateway: al igual que en los anteriores, añade una carga de trabajo innecesaria en red del cliente hasta el gateway.

Si tuviésemos que explicar brevemente lo que ha ocurrido en los últimos años respecto a la seguridad informática, podríamos decir que ha sido un año sin los sobresaltos de antes (los virus que se propagaban en muchos ordenadores y eran noticia en todos los periódicos) pero con un gran incremento en el número de nuevo malware detectado por las empresas del sector.

Así como a finales de los 90 y de 2000 a 2002 vivimos una explosión del fenómeno de los virus en Internet con epidemias masivas, en 2003 dicha tendencia comenzó a decaer.

Con el paso del tiempo, se comenzaron a observar dos hechos: las epidemias masivas eran menos frecuentes y menos impactantes y cada vez los virus eran amenazas más sofisticadas tecnológicamente. Además, sobre desde 2005, los objetivos de dichos ataques han pasado de ser masivos a ser dirigidos. De hecho ya no se producen alertas rojas provocadas por amenazas. Casi todas son naranjas e incluso ya hay alguna provocada por redes de bots.



Además, aparecen nuevos tipos de amenazas, que no son necesariamente virus, cuya principal virtud es la de pasar inadvertidas tanto a los usuarios como a las soluciones antimalware y que proporcionan a sus autores la posibilidad de tomar el control de ordenadores e introducirse en ellos sin que se entere nadie.

A este escenario le llamamos «La epidemia silenciosa» a diferencia de las «epidemias masivas» predominantes en la industria hasta 2005.

9.1_¿Por qué han cambiado las amenazas?

La evolución de las amenazas hay que buscarla en la evolución de sus autores. Éstos han pasado de actuar por mera curiosidad y de buscar la fama personal, a preocuparse por el beneficio económico personal y/o a formar parte de un complejo entramado de intereses empresariales, nacionales o políticos.

A la vez, también el grado de know-how y de conocimiento ha ido creciendo, y herramientas o técnicas que ayer estaban en manos sólo de los expertos, hoy alimentan las prácticas de los que empiezan en esta «profesión», elevando así la pericia general de todos ellos.

9.2_Los malos. Tipos

En este nuevo contexto, nos encontramos con diferentes figuras o arquetipos que, combinados con la motivación que los mueve, arroja una foto sobre el escenario actual.

Los vándalos. Habitualmente son los autores que acaban de iniciarse en el mundo de las amenazas de Internet movidos por la curiosidad. Aprenden en Internet, hacen pruebas, ven los resultados y, poco a poco, van aprendiendo. Su nivel de iniciación, sin embargo, es ahora más alto que hace unos años, dado que los expertos publican sus técnicas y logros y están al alcance de cualquiera en Internet. Al vándalo, al principio, le mueve la curiosidad, pero según va cogiendo confianza, comienza a ver las posibilidades de llegar a ser conocido gracias a sus «fechorías».

Intrusos. Básicamente, son hackers que tienen esta actividad como hobby y buscan la fama personal. En esta categoría también hay numerosos expertos o gurús. Son los que se «jactan» de haberse colado en el Banco Mundial. La mayoría de las veces no hacen nada más, porque el

propio reconocimiento de su acto es suficiente recompensa para ellos. Es normal que este tipo de perfil sea contratado en empresas de seguridad o que monten su propia empresa dedicada a las auditorías de seguridad, consultorías, etc.

Los ladrones. Son la evolución del hacker avanzado o experto que descubren que pueden conseguir un beneficio económico a sus actividades. Es la «Profesionalización» en el pleno sentido de la palabra. Así, la ganancia personal es lo que realmente mueve a este tipo de perfiles. Más tarde veremos cuáles son los modelos de negocio que permiten a estos autores convertir su hobby casi en una empresa organizada.

Los espías. Habitualmente, son autores de malware expertos o especialistas auténticos que ponen sus servicios a disposición del mejor postor. Aparte de la ganancia personal, habitualmente este tipo de prácticas forman parte de planes de espionaje industrial, político o, incluso, nacional.

9.3_Las nuevas amenazas

Anteriormente hablábamos de las nuevas amenazas que están apareciendo en el escenario actual. Para conocer un poco más estas nuevas amenazas, vamos a distinguir entre epidemias masivas y ataques dirigidos.

Definiremos epidemias masivas como aquellas dirigidas a infectar al mayor público posible. En su mayoría, estas amenazas eran gusanos que tenían capacidad de distribuirse por sí solos. Por lo tanto, este tipo de ataque busca perjudicar al máximo público posible y es una actividad propia de vándalos o intrusos, que buscan la fama personal.

Por el contrario, llamamos ataques dirigidos (targeted malware o targeted attacks) a aquellos realizados de manera silenciosa e imperceptible cuyo objetivo es una empresa en concreto, o un tipo de empresas, una persona, etc. No son ataques masivos, porque su objetivo no es alcanzar al mayor número posible de ordenadores.

El autor de este tipo de ataque puede utilizar cualquier tipo de malware para conseguir su objetivo: troyanos, bots, spyware, etc. Habitualmente, el autor es un ladrón o un espía, experto o especializado, una motivación económica, es decir, un tercero paga sus servicios.

Dado que el autor desarrolla su propia amenaza para conseguir su fin, ésta no se distribuye de forma masiva, sino que sólo se hace de forma di-

rigida y a un objetivo en concreto, y utilizan vanguardistas técnicas de ocultación (como rootkits), es prácticamente imposible que las soluciones de seguridad tradicionales sean capaces de conseguir un ejemplar para hacer la firma correspondiente y actualizar a todos los clientes.

Por lo tanto, para este tipo de ataques, los antivirus y otras soluciones de seguridad tradicionales son insuficientes.

Este tipo de amenazas comienzan a ser detectadas por algunas soluciones de seguridad, pero, aún así, existen cientos de miles de ejemplares que dan el control del PC al atacante sin que los usuarios ni siquiera lo sepan.

Los nuevos tipos de amenazas que utilizan los distintos autores de virus para llevar a cabo epidemias silenciosas o ataques dirigidos son:

- **Bot:** Es la contracción de un software robot. Un bot es un software que permite que el sistema sea controlado remotamente sin el conocimiento ni consentimiento del usuario.
- **Zombi:** Zombi: llamamos zombi a un sistema (un PC) controlado mediante la utilización de bots.
- **Botnet:** Es un grupo o una red de ordenadores zombis controlados por el «propietario» de los bots. El propietario de las redes de bots da instrucciones a los zombis. Estas órdenes pueden incluir la propia actualización del bot, la descarga de una nueva amenaza, el mostrar publicidad al usuario o el lanzar ataques de denegación de servicio, entre otras.
- **«Bot herder» o propietario de bot:** Es la persona o el grupo propietario que controla las redes de bot. También se les llama el «bot master» o el «zombi master».
- **Rootkit:** es una colección de herramientas que por sí mismas no son ni buenas ni malas. De hecho, se utilizan para muchas acciones lícitas. Sin embargo, un rootkit puede ser utilizado por un autor con algún propósito malo. También son comúnmente utilizados para ocultar otro tipo de amenazas. Existen ejemplos de rootkits que han estado ocultos durante años sin que los usuarios tuvieran consciencia del suceso.
- **Spear phishing:** Utiliza las técnicas del phishing pero se trata de un ataque dirigido lanzado contra un objetivo concreto. El autor que lance este tipo de ataque, nunca recurrirá al spam para conseguir una

avalancha masiva de datos personales de los usuarios. El hecho de que sea dirigido y no masivo implica una más rigurosa elaboración para dar mayor credibilidad, y la utilización más sofisticada de ingeniería social.

Los perjuicios que este tipo de amenazas y de ataques pueden causar en los ordenadores de los usuarios afectados son:

- **Riesgo de robo de información confidencial empresarial y económica y pérdida de la privacidad.** Es la evolución del espionaje industrial, sin necesidad de tener personas infiltradas que saquen la información de la propia empresa. Las consecuencias de este tipo de acción puede conllevar desde pérdidas económicas a, incluso, bancarrotas y otro tipo de consecuencias nefastas para la empresa.
- **Riesgos legales,** dado que si un atacante toma el control de un PC o de varios y lanza, por ejemplo, un ataque de denegación de servicios, la IP del atacante será la del usuario, que no tiene ningún conocimiento de esta acción.
- **Molestias causadas por la aparición de publicidad no deseada** y otro tipo acciones similares.
- **Ralentizaciones,** crashes, problemas con el ordenador en general, causados por las propias amenazas que pueden estar camufladas.

Los actores en la seguridad en la sociedad de la Información

Ignacio Alamillo
Director de Asesoramiento e investigación de la Agencia Catalana de Certificación (CATCert)

1_INTRODUCCIÓN

En este capítulo presentamos algunos actores relevantes en las políticas públicas de la seguridad de la información en los ámbitos internacional, europeo y del estado español.

Ante todo hay que advertir que no es posible presentar todos los organismos y las entidades que aportan materiales a la formación de las políticas públicas, por lo que se han escogido los más representativos de cada tipo de actuación.

También hay que indicar que se incluye una sección específica dedicada a los actores en el campo de la producción de normas y estándares que, pese a ser una actividad privada, es un instrumento esencial en las políticas públicas relativas a la seguridad de información.

2_ORGANISMOS INTERNACIONALES Y UNIÓN EUROPEA

2.1_Organización para la Cooperación y el Desarrollo Económico (OCDE)

La OCDE es un foro internacional que agrupa un importante número de estados y trata los desafíos económicos, sociales y de gobernanza de la globalización, y el análisis de las oportunidades que representa.

El papel de la OCDE en el desarrollo de políticas es bastante relevante, así como también la elaboración de encuestas y estudios comparativos entre países que lleva a cabo.

La actividad de la OCDE en relación con la seguridad de la información se ha centrado en la producción de guías sobre la protección de los datos de carácter personal y, más recientemente, en principios sobre la seguridad de la información y la cultura de la seguridad, y en la lucha con-

tra las comunicaciones comerciales no solicitadas (correo basura [spam]).

Hay dos grupos de trabajo importantes en seguridad de la información:

- **Grupo de trabajo de seguridad de la información y la privacidad.** Su misión es promover una aproximación global y coordinada en las políticas de la seguridad de la información, dado que generar confianza y seguridad en el uso de las tecnologías de la información y la comunicación (TIC) requiere transacciones fiables, seguras y privadas.
- **Fuerza de trabajo de comunicaciones comerciales no solicitadas.** Su misión es tratar el problema del correo basura, mediante una fuerte promoción de la cooperación internacional, y crear un conjunto de herramientas específicas (the Anti-Spam Toolkit), que incluye una guía de mejores prácticas para proveedores de servicios de Internet y que ayuda a los gobiernos, los reguladores y la industria al establecimiento de políticas efectivas para luchar contra esta problemática.

2.2_Consejo de Europa (CoE)

El CoE es una organización internacional cuyo objetivo es favorecer en Europa un espacio democrático y jurídico común, organizado alrededor del Convenio Europeo de Derechos Humanos y de otros textos de referencia sobre la protección del individuo.

El CoE tiene una dimensión paneuropea, que incluye 46 países miembros, 2 candidatos y 5 observadores (Vaticano, Estados Unidos, Canadá, Japón y México).

Uno de sus objetivos es buscar soluciones comunes a los problemas a los que se enfrenta la sociedad, como la discriminación de las minorías, la xenofobia, la intolerancia, la bioética y la clonación, el terrorismo, el tráfico de personas, la delincuencia organizada y la corrupción, la cibercriminalidad o la violencia sobre los menores.

La actividad reciente del CoE en relación con la seguridad de la información se ha desarrollado especialmente alrededor de la lucha contra la ciberdelincuencia, mediante la creación del importante Convenio Europeo 185, sobre cibercrimen, aprobado en Budapest el 23 de noviembre de 2001, y de su Protocolo Adicional 189, sobre criminalización de actos

de naturaleza racista y xenófoba llevados a cabo mediante sistemas informáticos, y que se aprobó en Estrasburgo el 28 de enero de 2003.

Asimismo, el CoE ha sido muy activo en materia de protección de datos personales, mediante instrumentos como el Convenio Europeo 108, sobre la protección de los individuos en relación con el procesamiento automático de datos personales, y su Protocolo Adicional 181, sobre autoridades de supervisión y flujos transfronterizos de datos.

También hay que hacer patente la importante Declaración del Comité de Ministros del CoE sobre los derechos humanos y la reafirmación de la Ley en la Sociedad de la Información, de 13 de mayo de 2005, en la que se reafirmó la idea de que la protección de datos personales es uno de los derechos esenciales que hay que preservar, con referencia al permanente equilibrio entre los instrumentos legales de intervención para el refuerzo de la seguridad y la privacidad de los individuos.

2.3_Unión Europea (UE)

La UE ha sido un jugador clave en el impulso de la seguridad de la información en el ámbito de la administración electrónica, como se puede ver a continuación.

Los últimos cinco años han estado marcados por una rápida y muy importante evolución de la seguridad y confianza, que se ha convertido en 2006 en una prioridad política y estratégica para la sociedad de la información y, en especial, para la administración electrónica.

La política de la UE está recogida de una forma particularmente clara en la reciente Comunicación de la Comisión al Consejo, en el Parlamento Europeo, en el Comité Económico y Social, y en el Comité de las Regiones, «Una estrategia para una sociedad de la información segura. Diálogo, asociación y potenciación», COM (2006) 251, de 31 de mayo de 2006, dentro del marco estratégico 2010, que revisa el estado actual de las amenazas a la seguridad de la sociedad de la información y determina nuevas acciones para mejorar el nivel general de seguridad de las redes y la información.

En esta Comunicación se reconoce que la seguridad es un reto para todos, incluyendo a las administraciones públicas, que deben afrontar la seguridad de sus sistemas, no sólo para proteger la información del sector público, sino también para dar ejemplo de buenas prácticas al resto de agentes.

Uno de los mecanismos más importantes que se identifican en la citada Comunicación para mejorar el nivel de seguridad es el conocimiento, especialmente en un entorno cada vez más diverso, abierto e interoperable, así como generar una cultura de la seguridad generalizada.

En este contexto, la Comisión invita a los estados miembro a, entre otras, las siguientes acciones siguientes:

- Promover campañas de sensibilización sobre las virtudes, los beneficios y ventajas asociadas a la adopción de unas tecnologías, prácticas y comportamientos efectivos en relación con la seguridad.
- Impulsar el despliegue de servicios de administración electrónica destinados a comunicar y fomentar las buenas prácticas de seguridad, que después podrían extenderse a otros sectores.

Asimismo, en esta Comunicación se invita, entre otras acciones, a combatir el robo de la identidad y otros ataques contra la privacidad.

En el mismo contexto hay que situar a la Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social y al Comité de las Regiones, «Sobre lucha contra el *spam*, el software espía y el software malicioso», COMO (2006) 688, de 15 de noviembre de 2006, que identifica líneas de actuación para combatir estas amenazas a la seguridad.

Las acciones que se proponen en esta Comunicación incluyen:

- El refuerzo del derecho comunitario.
- La aplicación del marco regulativo vigente para combatir el problema.
- La cooperación dentro y entre los estados miembro.
- El diálogo político y económico con terceros Estados.
- El fomento de las iniciativas de la industria.
- Las actividades de I+D.

La UE también ha tratado la cuestión de la protección de las infraestructuras críticas de la información, por ejemplo, la Comunicación de la Comisión en el Consejo y en el Parlamento Europeo, «Protección de las infraestructuras críticas en la lucha contra el terrorismo», COM (2004) 702, de 20 de octubre de 2004, o el Libro verde sobre una programa europeo para la protección de las infraestructuras críticas, COM (2005) 576, de 17 de noviembre de 2005 y la reciente Propuesta de directiva del Consejo sobre la identificación y designación de las infraestructuras críti-

cas europeas y la evaluación de la necesidad de mejorar su protección, COM (2006) 787, de 12 de diciembre de 2006.

Tampoco se puede olvidar la importante actividad de la UE en materia de contenidos en la red Internet.

Otra gran línea de actuación de la UE, que veremos en el capítulo tercero de esta segunda parte, incluye la gestión de identidades, la firma electrónica y la privacidad.

2.4_Agencia Europea de Seguridad de las Redes y de la Información (ENISA)

La ENISA es una agencia de la UE creada para impulsar el funcionamiento del mercado interior prestando asesoramiento y asistencia a los estados miembros, a los órganos de la UE y a las organizaciones empresariales, con el fin de dotar las redes y la información de un nivel alto y eficaz de seguridad.

La ENISA actúa igualmente como centro de competencia para los estados miembros y las instituciones comunitarias y facilitando el intercambio de información y la cooperación.

Algunas de las actividades más relevantes de la ENISA han sido las siguientes:

- Catálogo de participantes en seguridad de la información.
- Catálogo de centro de respuestas a emergencias informáticas.
- Guías sobre programas de concienciación de la seguridad.
- Estudio sobre la seguridad de las comunicaciones electrónicas y el correo basura.
- Inventario sobre actividades y normas de seguridad.
- Asistencia a la Comisión Europea y autoridades de algunos estados miembros en aspectos sobre seguridad de la información, niveles de autenticación, firma electrónica y otros.

2.5_Cámara de Comercio Internacional (ICC)

La ICC es una organización internacional abierta a empresas, profesionales y cámaras de comercio, que actúa en defensa de los intereses de estos colectivos de forma coordinada con otros organismos internacionales. Se

fundó en 1919, y su misión es promover el comercio internacional, eliminando los obstáculos y las distorsiones; promover un sistema de economía de mercado basado en el principio de libre comercio y de competencia leal entre los participantes; y fomentar el crecimiento económico de los países desarrollados y en vías de desarrollo por igual, con una orientación a una mejor integración de todos los países en la economía mundial.

La actividad de la ICC en relación con la seguridad de la información incluye:

- GUIDEC, que son unas guías para la llevar a cabo comercio electrónico seguro, incluyendo los aspectos de autenticación, firma electrónica, confidencialidad y otros (versiones 1997 y 2001).
- Recomendaciones sobre cibercriminalidad en los estados signatarios del Convenio 185 del CoE y su Protocolo Adicional (2003).
- Posición común con otras organizaciones representativas de intereses empresariales sobre el almacenamiento de datos de tráfico para propósitos legales (2003).
- Guía de seguridad de la información para ejecutivos, publicada conjuntamente con BIAC de la OCDE (2003).
- Posición oficial en relación con las comunicaciones comerciales no solicitadas y el correo basura (2004).
- Posición oficial con recomendaciones a los estados en relación con los principios que deberán guiar la normativa legal sobre cumplimiento regulativo de seguridad de la información (2006).

Hay que mencionar a la Federación Mundial de Cámaras, una división de la ICC especializada en esta materia que agrupa todas las cámaras de comercio que participan en la ICC y que ha creado, conjuntamente con la Cámara de Comercio de París, la Red Mundial de Cámaras, con interesantes proyectos en seguridad y confianza, como los siguientes:

- ChamberTrust, un sello de confianza que consiste en un sistema de validación internacional con una solución de marketing incluida, a través de servicios de la ICC.

  Con ChamberTrust, las Cámaras de Comercio verifican una información objetiva en relación con una empresa (su existencia, la propiedad de la página web, los productos, las actividades principales y secundarias, etc.), y no se incluye información subjetiva sobre el rendimiento

de la empresa. ChamberTrust ayuda a superar los problemas del anonimato, la confianza y la visibilidad de la marca en la red.

ChamberTrust se encuentra dentro del directorio global de Cámaras operado por la Red Mundial de Cámaras, que incluye una descripción del negocio, la posibilidad de que la empresa publique su catálogo de productos, y enlaces directos en la página web y en el almacén web de la empresa.

- Chamber e-Vault, un depósito seguro de ficheros de empresa, para el que se emite de manera automática un certificado digital de notaría, custodiado por la Red Mundial de Cámaras y despachos de abogados.

  Cada cuenta de empresa permite la creación de archivadores seguros, de forma que cada fichero almacenado puede ser marcado con descripciones multilingües para la búsqueda posterior de los contenidos.

- ChamberSign, un programa de certificación de firma electrónica establecido por las cámaras de comercio con la voluntad de crear una arquitectura global para el comercio electrónico seguro internacional, así como para promover la tecnología de autenticación robusta y de firma digital y para obtener el reconocimiento internacional y la interoperabilidad.

  ChamberSign opera principalmente en Europa, mediante socios en nueve estados incluyendo el Estado español, con la participación del Consejo Superior de Cámaras de Comercio, Industria y Navegación de España y su iniciativa empresarial Camerfirma.

3_ORGANISMOS DE DESARROLLO DE ESTÁNDARES

3.1_Organización Internacional de Estandardización (ISO) y Comisión Electrotécnica Internacional (CEI)

La ISO y el CEI forman el sistema especializado de normalización internacional, en el cual participan las entidades nacionales de normalización que son miembros, a través de comités técnicos establecidos para tratar materias específicas. Otras organizaciones, públicas y privadas, también participan en los trabajos de forma habitual, mediante acuerdos de colaboración con la ISO y el CEI.

La actividad de la ISO/CEI en relación con la seguridad de la información ha sido ingente, mediante un comité técnico conjunto (JTC) 1. Los sub-

comités (SC) más importantes que tienen responsabilidades de seguridad de la información son los siguientes:

- **ISO/CEI JTC 1 SC 6: telecomunicaciones e intercambio de información entre sistemas.** Su misión es la normalización de las telecomunicaciones que tratan el intercambio de información entre sistemas abiertos, incluyendo aspectos de la seguridad.
- **ISO/CEI JTC 1 SC 27:** técnicas de seguridad de la información. Su misión es la normalización de técnicas y métodos genéricos de seguridad de la información, incluyendo los siguientes aspectos:
  - Identificación de requisitos genéricos para servicios de seguridad de sistemas de información, incluyendo las metodologías de requisitos.
  - Desarrollo de mecanismos y técnicas de seguridad, incluyendo los procedimientos de registro y las relaciones entre los componentes de seguridad.
  - Desarrollo de guías de seguridad, como por ejemplo documentos interpretativos, de análisis de riesgo y otros. Aquí hay que mencionar la muy relevante serie 27000 de seguridad (que incluye la norma ISO 17799 a partir de 2007).
  - Desarrollo de documentación y normas de apoyo a la gestión, como por ejemplo, terminología y criterios de evaluación de la seguridad.
  - Normalización de algoritmos criptográficos para la integridad, la autenticación y la irrefutabilidad (no repudio), y la confidencialidad de la información, de acuerdo con políticas aceptadas internacionalmente.

  Actualmente, el SC 27 dispone de los siguientes grupos de trabajo:
  - WG 1: sistemas de gestión de la seguridad de la información.
  - WG 2: criptografía y mecanismos de seguridad.
  - WG 3: criterios de evaluación de la seguridad.
  - WG 4: servicios y controles de seguridad.
  - WG 5: tecnologías de gestión de identidad i privacidad (incluyendo la biometría).
- **ISO/CEI JTC 1 SC 37 Biometrías.** Su misión es la normalización de las tecnologías de biometría genética perteneciente a los seres humanos para ofrecer apoyo a la interoperabilidad y al intercambio de

datos entre aplicaciones y sistemas. Complementa el trabajo de otros SC en biometría, como el SC 17, que aplica tecnologías biométricas a la identificación personal y a las tarjetas, o el SC 27, que trabaja en la protección de los datos biométricos, así como la evaluación y las pruebas de seguridad biométrica.

Actualmente, el SC 37 dispone de los siguientes grupos de trabajo:

– WG 1: vocabulario armonizado sobre biometría.

– WG 2: interfaces técnicas biométricas.

– WG 3: formatos de intercambio de datos biométricos.

– WG 4: arquitectura funcional biométrica y perfiles relacionados.

– WG 5: pruebas e informes biométricos.

– WG 6: aspectos sociales e internacionales.

3.2_Unión Internacional de Telecomunicaciones, sección de telecomunicaciones (ITU-T)

La ITU-T actúa como un foro en el cual los gobiernos y el sector privado desarrollan normas para las redes y los servicios globales de telecomunicaciones. Es una de las secciones de la ITU, un organismo internacional del sistema de las Naciones Unidas.

La actividad de la ITU-T en relación con la seguridad de la información ha sido muy importante y afecta prácticamente a la totalidad de sistemas empleados en telecomunicaciones, frecuentemente en colaboración con otras organizaciones de desarrollo de normas.

Ya hace tiempo que la ITU-T ha desarrollado un conjunto de recomendaciones sobre seguridad: la Recomendación X.800 es un documento de referencia en la arquitectura de seguridad para la interconexión de sistemas abiertos, y la serie X.810-X.816 define un marco de seguridad para sistemas abiertos, publicado conjuntamente con la ISO/CEI, que cubre la autenticación, el control de acceso, la irrefutabilidad (no repudio), la confidencialidad, la integridad y las alarmas de seguridad y auditoría.

Más recientemente, se ha desarrollado la Recomendación X.805 para describir la arquitectura de seguridad para sistemas que ofrecen comunicaciones extremo a extremo, tomando en consideración las nuevas amenazas y vulnerabilidades que resultan en torno a múltiples redes y proveedores de sistemas.

Por otro lado, la ITU-T produjo la Recomendación X.509 sobre certificados de clave pública y de atributos, documento fundacional en los sistemas de firma electrónica.

Adicionalmente a estas recomendaciones, la ITU-T ha desarrollado otras provisiones de seguridad, relativas a sistemas de telecomunicaciones, como por ejemplo en Voz sobre IP empleando H.323 o IPCablecom, transmisión segura de fax o gestión de red.

Se puede acceder a una visión más detallada de los trabajos de normalización de seguridad en la que ha participado la ITU a través del informe sobre seguridad en las telecomunicaciones y tecnologías de la información publicado por la ITU en 2006.

Adicionalmente, la ITU ha estado muy involucrada en grupos de estudio específicos sobre la prevención técnica de las comunicaciones comerciales no solicitadas (correo basura) y en la lucha contra la ciber-criminalidad.

El grupo de trabajo más importante con responsabilidades de seguridad de la información es el Study Group 17, sobre seguridad, lenguajes y software de telecomunicaciones. Su misión es elaborar estudios sobre seguridad, la aplicación de comunicaciones de sistemas abiertos, incluyendo redes y directorios, y sobre lenguajes técnicos, el método para utilizarlos y otros aspectos del software de los sistemas de telecomunicaciones.

El grupo 17 ha sido nombrado líder en relación con todos los aspectos de seguridad dentro de la ITU-T, que coordinan con el resto de grupos dentro la ITU-T mediante un proyecto de seguridad. Actualmente, disponen de los siguientes grupos de trabajo:

– WP1 - Tecnologías de sistemas abiertos.

– WP2 - Seguridad de telecomunicaciones.

– WP3 - Lenguajes y software de telecomunicaciones.

3.3_Grupo Directivo de Seguridad de las Redes y la Información (ICTSB)

El ICTSB es un grupo de organizaciones que colaboran en la normalización de las TIC llevando a cabo propuestas y recomendaciones. Sus miembros se incluyen en la Comisión Europea, en las patronales y los

sindicatos europeos, y en las organizaciones europeas que desarrollan estándares (Comité Europeo de Normalización [CEN], Comité Europeo de Normalización Electrotécnica [CENELEC], e Instituto Europeo de Normas de Telecomunicaciones [ETSI]).

Hay que mencionar dos grupos relevantes en relación con la seguridad de la información:

- **La Iniciativa Europea de Normalización de la Firma Electrónica (EESSI).** El ICTSB se involucró activamente en el área de las firmas electrónicas entre 1999 y 2004 mediante este grupo, que recibió el encargo de coordinar las actividades de normalización que se realizaron con la Directiva 1999/93/CE sobre firma electrónica. Las actividades de normalización indicadas se desarrollaron en el CEN/ISSS (Information Society Standardization System) y en el ETSI. Esta tarea de coordinación ha sido asumida por el NISSG (Grupo Directivo de Seguridad de Redes y de la Información).
- **El Grupo Directivo de Seguridad de Redes y de la Información (NISSG).** El NISSG se formó el año 2004 con la misión de garantizar la implementación de los requisitos de normalización de seguridad de la información identificados en el informe especial ETSI SR 002 298, que contenía la respuesta del CEN y del ETSI a la «Comunicación de la Comisión en el Consejo, en el Parlamento Europeo, en el Comité Económico y Social y en el Comité de las Regiones: Seguridad de la información y las Redes: propuesta para una aproximación a una política europea».

  Recientemente el NISSG ha finalizado una segunda versión de este estudio.

El ICTSB también participa en otros trabajos, incluyendo el comercio electrónico, la protección de datos personales, los servicios de red, los servicios de localización o las tarjetas de identificación.

3.4_Instituto Europeo de Normas de Telecomunicaciones (ETSI)

El ETSI es una organización independiente, sin ánimo de lucro, que tiene la misión de producir normas de telecomunicaciones. Está formado por 688 miembros de 55 estados, incluyendo fabricantes, operadores de red, administraciones públicas, proveedores de servicios, organismos de búsqueda y usuarios de tecnologías de TIC.

Además, es el organismo oficialmente responsable en materia de normalización de las TIC en Europa, aunque el CEN también desempeña un papel muy importante en esta tarea.

Las tecnologías normalizadas por el ETSI incluyen las telecomunicaciones, la radiodifusión (incluyendo la televisión digital terrestre [TDT], por ejemplo), el transporte inteligente o los dispositivos médicos.

La actividad del ETSI en relación con la seguridad de la información ha sido bastante importante, principalmente por los aspectos de seguridad de las telecomunicaciones en general y de las comunicaciones móviles de segunda y tercera generación en particular.

Asimismo, el ETSI ha tratado los aspectos de seguridad de la TDT, y ha tenido un papel muy relevante en el desarrollo de las normas aplicables a la firma electrónica reconocida y a los prestadores de servicios de certificación.

3.5_Comité Europeo de Normalización (CEN)

El CEN es una organización que produce normas europeas en varios ámbitos, entre los cuales están las TIC.

La actividad del CEN en relación con la seguridad de la información se desarrolla mediante el CEN/ISSS, que realiza las siguientes actividades:

- **Talleres CEN/ISSS.** El CEN organiza talleres, que acercan a los consorcios de la industria a la normalización europea dentro de áreas específicas de interés con el objetivo de producir acuerdos de talleres CEN (CWA), que son especificaciones técnicas abiertas y basadas en el consenso.

  Se realizan trabajos en las áreas de negocio y comercio electrónico, por ejemplo el taller de facturación electrónica o el taller de catalogación y clasificación electrónica.

  El taller de protección de datos y privacidad (2003-2007) ofrece apoyo a la implementación de la Directiva de protección de datos y a las legislaciones nacionales correspondientes.

  El taller de autenticación electrónica (2003-2005) ha hecho contribuciones en el área de las tarjetas inteligentes y las aplicaciones de gobierno electrónico, y también ha aportado un documento de visión estratégica titulado «Hacia un ID electrónico para el ciudadano europeo», que con-

tiene un enfoque técnico de la cuestión, amenazas y oportunidades en esta área.

La firma electrónica ha sido tratada en un taller específico, que finalizó en 2003. Se han desarrollado diversos CWA, algunos de los cuales se mantienen al día por el CEN/ISSS, el ETSI/ESI y el CEN/TC 224. Este Comité Técnico 224 (identificación personal, firma electrónica y tarjetas y sus sistemas y operaciones relacionados) trabaja de forma particular en el área de las tarjetas inteligentes. La Decisión de la Comisión Europea de 14 de julio de 2003 identifica los CWA 14169 y CWA 14167-1/2 como estándares generalmente reconocidos de firma electrónica.

- **Grupos de enfoque CEN/ISSS.** Un grupo de enfoque CEN/ISSS trata con una temática específica de normalización y produce informes, descripciones generales y recomendaciones, y opera de forma previa a la normalización formal. El CEN/ISSS tiene varios grupos relativos a la seguridad de la información:
  - Grupo de enfoque en biometría.
  - Grupo de enfoque en administración electrónica, especialmente orientado a la interoperabilidad.
  - Grupo de enfoque en salud electrónica.
  - Grupo de enfoque en negocio electrónico.
  - Grupo de enfoque en facturación electrónica.
  - Grupo de enfoque en gestión de derechos de autor digital.
- El grupo de trabajo CEN BT/WG 161, denominado protección y seguridad del ciudadano, se encarga del seguimiento de las actividades de normalización, y la necesidad de nuevas actividades, en el ámbito de las infraestructuras críticas o los servicios de emergencia.

3.6_Fuerza de trabajo de ingenieros de Internet (IETF)

La IETF es la comunidad internacional de diseñadores de redes, operadores, productores de software y buscadores más importante que trabaja en el funcionamiento correcto y la evolución técnica de Internet, comunidad que se encuentra abierta a cualquier individuo que quiera participar.

Los trabajos técnicos de la IETF se llevan a cabo dentro de grupos de trabajo, que se organizan por materias en diferentes áreas (por ejemplo, direccionamiento, transporte y seguridad). La mayor parte del trabajo se

desarrolla a través de listas de correo, y con la realización de tres reuniones presenciales anuales.

La actividad de la IETF en relación con la seguridad de la información en Internet es de las más importantes, y se gestiona dentro del área de seguridad. Está formada por los directores de área, un consejo de dirección que incluye los jefes de los grupos de trabajo y asesores específicamente nombrados, y es asistida y asesorada por un grupo específico (SAAG).

Actualmente, los grupos de trabajo del área de seguridad son los siguientes:

- Better-Than-Nothing Security WG
- Domain Keys Identified Mail WG
- EAP Method Update WG
- Extended Incident Handling WG
- IETF Open PGP WG
- IETF X.509 Public Key Infrastructure WG
- IETF Transport Layer Security (TLS) WG
- Integrated Security Model for SNMP WG
- Kerberos WG
- Kitten (GSS-API Next Generation) WG
- Long-Term Archive and Notary Services WG
- Multicast Security WG
- Profiling Use of PKI in IPSEC WG
- Secure Mime WG
- Securely Available Credentials WG
- Security Issues in Network Event Logging (SYSLOG) WG
- Secure Shell WG
- Simple Authentication and Security Layer WG
- The XML Digital Signature WG

3.7_Consorcio World Wide Web (W3C)

El W3C es un consorcio internacional en el que las organizaciones miembro, el personal a tiempo completo y el público en general trabajan

conjuntamente para desarrollar normas web. La misión del W3C es guiar la web hacia su máximo potencial mediante el desarrollo de protocolos y pautas que aseguren su futuro crecimiento.

El W3C organiza los trabajos en actividades y dispone de una actividad específica en seguridad de la información. Actualmente, el trabajo de esta actividad sigue dos líneas:

- Grupo de trabajo contexto de seguridad de la web: trata con los retos de los usuarios con tecnologías de seguridad ampliamente implantadas, como TLS (protección a nivel de transporte), dado que, aunque estas tecnologías funcionan correctamente, las estrategias de los atacantes persiguen saltárselas en lugar de romperlas mediante engaños a los usuarios que, por el hecho de no ser conscientes del funcionamiento de las tecnologías, son defraudados fácilmente.
- El Grupo de trabajo de mantenimiento de especificaciones de seguridad: se dedica a mantener las especificaciones de seguridad XML vigentes, documentar mejores prácticas sobre su uso y evaluar la necesidad de realizar más trabajos en esta área.

Les especificaciones de seguridad publicadas por el W3C incluyen:

– Firmas XML

– XML Canónico

– Cifraje XML

– Gestión de claves en XML

3.8_ASIS

OASIS es un consorcio internacional sin ánimo de lucro que persigue el desarrollo, la convergencia y la adopción de estándares de negocio electrónico. El consorcio produce la mayoría de estándares sobre servicios web, conjuntamente con estándares para la seguridad de los mismos. OASIS tiene más de 600 organizaciones de más de 100 estados que participan en este proceso.

La actividad de OASIS en relación con la seguridad de la información es muy completa. Forman parte los siguientes comités técnicos:

- Integración de servicios de aseguramiento de la identidad con biometría (BIAS): define los métodos para emplear la autenticación basada

en biometría en servicios web transaccionales y arquitecturas orientadas a servicios.

- Servicios de firma digital (DSS): define una interfaz XML para procesar firmas electrónicas para servicios web y otras aplicaciones.
- Infraestructura de gestión de claves empresarial (EKMI): define protocolos de gestión de claves simétricas.
- Lenguaje extensible de marcas de control de acceso (XACML): trabaja en la representación y la evaluación de políticas de control de acceso.
- Servicios de aprovisionamiento: ofrece un marco de trabajo en XML para gestionar el aprovisionamiento y la asignación de información de identidad y de recursos del sistema dentro de organizaciones y entre éstas.
- Adopción de Infraestructura de clave pública (PKIA): aboga por el uso de los certificados digitales como base para el acceso a los recursos de red y para llevar a cabo la realización de transacciones electrónicas.
- CTJ: coordina las diversas actividades de OASIS en seguridad.
- Servicios de seguridad (SAML): define y mantiene un marco de trabajo en XML para crear e intercambiar información de seguridad en línea.
- Seguridad en servicios Web (WSS): ofrece una base técnica para implementar funciones de seguridad en mensajería SOAP.
- Federación de servicios web (WSFED): trabaja en la extensión de la gestión de identidad para permitir federaciones de confianza entre organizaciones.
- Intercambio seguro de servicios web (WS-SX): define políticas y extensiones en WSS para permitir el intercambio fiable de múltiples mensajes SOAP.

4_ESTADO ESPAÑOL

4.1_Ministerio de Industria, Turismo y Comercio

El Ministerio de Industria, Turismo y Comercio, a través de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, ha recibido la dirección estratégica de la ejecución del Plan Avanza, aprobado por Acuerdo del Consejo de Ministros de 4 de noviembre de 2005.

El Plan Avanza tiene por finalidad el desarrollo de la sociedad de la información, dentro de un escenario temporal 2006-2010, para la

convergencia en Europa y entre comunidades autónomas y ciudades autónomas, incluyendo una línea de actuación específica en materia de seguridad y confianza.

Dentro de esta actividad hay que inscribir la actividad de Red.es y RedIRIS, así como la del Instituto Nacional de Tecnología de la Comunicación (INTECO), que veremos a continuación.

4.2_Red.es y RedIRIS

Res.es es una entidad pública empresarial adscrita al Ministerio de Industria, Turismo y Comercio cuyas funciones principales son las siguientes:

- Impulsar el desarrollo de la seguridad de la información mediante la ejecución de programas definidos en el Plan Avanza para la convergencia en Europa y entre comunidades autónomas.
- Analizar la sociedad de la información a través del Observatorio de las Telecomunicaciones y de la Sociedad de la Información.
- Ofrecer asesoramiento y apoyo específico a la Administración General del Estado.
- Gestionar el registro de nombres de dominio .es.

En las cuestiones relativas a la seguridad tecnológica y de la sociedad de la información, resulta necesario definir un plan estratégico y un modelo para la implantación de un centro nacional de seguridad que incluya la puesta marcha de un centro demostrador de seguridad para la pyme con el objetivo de: (i) realizar pruebas y comparaciones de varios tipos de productos de seguridad; (ii) servir de plataforma de pruebas y apoyo a otros centros como el Centro de Respuesta a Incidentes en Tecnologías de la Información y el Observatorio de Seguridad; y (iii) potenciar el uso de las tecnologías de seguridad de la información entre las pymes españolas e impulsar la visibilidad internacional de la tecnología española de seguridad de la información.

Por otro lado, se considera necesario realizar una investigación sobre usuarios de Internet con la finalidad de hacer un estudio sobre incidencia y confianza de los usuarios en la red. De esta manera se persigue impulsar el conocimiento y el seguimiento de los principales indicadores y políticas públicas relacionados con la seguridad de la información y la confianza; la generación de una base de datos que permita el análisis y

evaluación de la seguridad y la confianza con una perspectiva temporal, y, finalmente, elaborar y presentar informes en materia de seguridad, que sirvan de apoyo a la toma de decisiones por parte de la Administración en materia de seguridad.

Red.es ha de ejecutar las siguientes actuaciones en materia de seguridad:

- En relación con el centro demostrador de seguridad de la información para la pyme, la implantación y el mantenimiento de un centro demostrador capaz de realizar demostraciones de seguridad para entornos empresariales, llevar a cabo pruebas y comparaciones de varios productos de seguridad sobre diversidad de plataformas, aplicaciones y canales de comunicación, apoyar a otros centros relacionados con la seguridad tecnológica y realizar tareas de difusión que impulsen la visibilidad nacional e internacional de la tecnología española de seguridad.
- En relación con la investigación sobre usuarios de Internet, un estudio sobre incidencia y confianza de los usuarios a la red.

Hay que mencionar que la actividad de Red.es se realiza en régimen de encargo de gestión por parte de la Secretaría del Estado de Telecomunicaciones y para la Sociedad de la Información del Ministerio de Industria, Turismo y Comercio, publicada por la Resolución de 1 de febrero de 2007.

Por otro lado, Red.se gestiona RedIRIS y participa en el INTECO. RedIRIS es la red nacional de investigación y desarrollo (I+D), que presta servicios de seguridad a la comunidad científica, incluyendo:

- El servicio de seguridad de RedIRIS (IRIS-CERT), que tiene como misión la detección de problemas que afecten a la seguridad de las redes de centros de RedIRIS, así como la actuación coordinada con estos centros para solucionar estos problemas. También se realiza una tarea preventiva que consiste en, avisar con tiempo de problemas potenciales, ofrecer asesoramiento a los centros, organizar actividades de acuerdo con estos, y otros servicios complementarios.
- Servicios de infraestructura de clave pública (PKI) para la comunidad RedIRIS, incluyendo certificados de servidores seguros y certificados de redes Grid.
- Servicios de control de acceso y autorización, mediante el software PAPI.

4.3_Instituto Nacional de Tecnología de la Comunicación (INTECO)

El INTECO, promovido por el Ministerio de Industria, Turismo y Comercio, y participado por Red.es, es una plataforma para el desarrollo de la sociedad del conocimiento mediante proyectos en el ámbito de la innovación y la tecnología, incluyendo iniciativas de seguridad tecnológica, accesibilidad e inclusión a la sociedad digital, así como soluciones de comunicación para particulares y empresas.

La actividad del INTECO en relación con la seguridad de la información incluye los siguientes proyectos:

- Centro de Respuesta a Incidentes en Tecnologías de la Información para pymes: tiene como misión principal conseguir un desarrollo sólido del tejido empresarial español mediante la provisión a las pymes de servicios reactivos, preventivos y formación en materia de seguridad.
- Centro de Alerta Rápida Antivirus (CATA): tiene como misión principal la concienciación en materia de seguridad, ofreciendo desde el año 2001 alertas, información, herramientas de protección gratuitas e informes diarios de seguridad sobre los últimos códigos maliciosos aparecidos en la Red desde 2001.
- Centro de información para la difusión de la cultura de la seguridad. Tiene como misión principal:
  - Poner en marcha y operar un portal de difusión y divulgación de información en materia de seguridad de la información.
  - Elaborar contenidos y guías prácticas en materia de seguridad de la información, en colaboración con agentes relevantes en este ámbito.
- Observatorio de la Seguridad de la Información: tiene como misión principal analizar, describir, asesorar y difundir la cultura de la seguridad y la confianza en la sociedad de la información, mediante la generación de conocimiento especializado en la materia, y la elaboración de recomendaciones y propuestas que permitan definir tendencias válidas para la toma de decisiones en el ámbito de la seguridad.
  - El Observatorio deberá ser un centro de referencia para el análisis y el seguimiento de la confianza en la sociedad de la información en España, y ha de elaborar, recoger, sintetizar y sistematizar indicadores.
  - Por otro lado, se debe generar y difundir conocimiento especializado como mínimo en las siguientes áreas clave de la seguridad de la información:

- Seguridad de la firma electrónica y de la identidad digital.
- Medidas de protección ante riesgos de seguridad de la información.
- Tecnologías de gestión de los derechos de autor en el ámbito digital (DRM).
- Otras tecnologías y herramientas de seguridad disponibles.

Hay que indicar que la actividad del INTECO se realiza en régimen de encargo de gestión por parte de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información del Ministerio de Industria, Turismo y Comercio, publicada por la Resolución del 1 de febrero de 2007. Este encargo de gestión también incluye el desarrollo de un sistema de intermediación de servicios electrónicos entre administraciones públicas.

4.4_Ministerio de Administraciones Públicas

El Ministerio de Administraciones Públicas impulsa los aspectos de seguridad del procedimiento administrativo basado en tecnologías de la información (medios electrónicos, informáticos y telemáticos) por parte de las administraciones públicas.

En este sentido, hay que mencionar la tarea que viene llevando a cabo en la difusión de la cultura de la seguridad, mediante la importante tarea del Consejo Superior de Informática, hoy Consejo Superior de Administración Electrónica, que ha avanzado en la definición inicial del esquema nacional de evaluación de la seguridad de la información y en la publicación de criterios y normas de seguridad de la información en el ámbito de la Administración General del Estado.

Más recientemente, hay que considerar la Ley de acceso electrónico de los ciudadanos a las administraciones públicas, que contiene importantes novedades en cuanto a la seguridad, identificación y firma electrónica en el ámbito de la llamada *administración electrónica.*

4.5_Centro Criptológico Nacional - Centro Nacional de Inteligencia (CCN-CNI)

El secretario de Estado, como director del Centro Nacional de Inteligencia (CNI) y director del Centro Criptológico Nacional (CCN), es la autoridad responsable de coordinar la acción de los diferentes organis-

mos de la Administración que utilizan medios o procedimientos de cifraje, garantizar la seguridad de las tecnologías de la información en este ámbito, informar sobre la adquisición coordinada del material criptológico y formar al personal de la Administración especialista en este campo.

El director del CCN es la autoridad de certificación de la seguridad de las tecnologías de la información (<WWW.oc.ccn.cni.se>) y la autoridad de certificación criptológica (<WWW.ccn.cni.se>). Asimismo, es responsable de velar por el cumplimiento de la normativa relativa a la protección de la información clasificada, en los aspectos de los sistemas de información y telecomunicaciones, de acuerdo con los artículos 4.e) y f) de la Ley 11/2002, de 6 de mayo.

El CCN se encuentra adscrito al CNI y comparte con éste medios, procedimientos, normativa y recursos. Dentro de su ámbito de actuación, el CCN realiza las funciones siguientes:

- Elaborar y difundir normas, instrucciones, guías y recomendaciones para garantizar la seguridad de los sistemas de las TIC de la Administración. Las acciones derivadas del desarrollo de esta función deben ser proporcionales a los riesgos a los que esté sometida la información procesada, almacenada o transmitida por los sistemas (<http://www.ccn.cni.se>).
- Formar al personal de la Administración especialista en el campo de la seguridad de los sistemas de las TIC.
- Constituir el organismo de certificación del esquema nacional de evaluación y certificación de la seguridad de las tecnologías de la información, aplicable a los productos y los sistemas en su ámbito (<http://www.oc.ccn.cni.se>).
- Valorar y acreditar la capacidad de los productos de cifraje y de los sistemas de las tecnologías de la información, que incluyan medios de cifraje para procesar, almacenar o transmitir información de forma manera segura.
- Coordinar la promoción, el desarrollo, la obtención, la adquisición y la implementación de la tecnología de seguridad de los sistemas antes mencionados.
- Velar por el cumplimiento de la normativa relativa a la protección de la información clasificada en su ámbito de competencia (por ejemplo, información de seguridad OTAN).

- Establecer las relaciones necesarias y firmar los acuerdos pertinentes con organizaciones similares de otros estados para el desarrollo de las funciones mencionadas.

Dentro de las actividades del CCN, hay que indicar el CCN-CERT, el equipo de respuesta a incidentes de seguridad de la información, que tiene como objetivo principal la mejora del nivel de seguridad de los sistemas de información en las administraciones públicas del Estado español.

La misión del CCN-CERT es ser el centro de alerta y respuesta a incidentes de seguridad, y ayudar a las administraciones públicas a responder de forma más rápida y eficiente ante las amenazas de seguridad que afectan a sus sistemas de información, a través de dos grandes líneas de actuación:

- La prestación de servicios de información, como los servicios de alertas de nuevas amenazas.
- La realización de tareas de búsqueda, formación y divulgación de la seguridad de la información.

4.6_Cámaras de Comercio, Navegación e Industria

La actividad de las cámaras en relación con la seguridad de la información se ha centrado en el suministro de herramientas de seguridad a las empresas y, de forma particular, servicio de certificación digital de la identidad corporativa, a través de su iniciativa Camerfirma.

Camerfirma está asociada al proyecto ChamberSign, y actualmente Camerfirma ofrece los siguientes tipos de certificados:

- Certificados de pertinencia a empresa
- Certificados de representante (con todos los poderes)
- Certificados de apoderado
- Certificados de persona jurídica
- Certificados para factura electrónica
- Certificados de servidor seguro
- Certificados de sello de empresa
- Certificados de firma de código

Asimismo, ofrece servicios complementarios, como el sellado de fecha y hora, la validación de certificados y producto y herramientas para firmar.

4.7_Asociación Multisectorial de Empresas Españolas de Electrónica y Comunicaciones (ASIMELEC)

La ASIMELEC agrupa a fabricantes, comercializadores, distribuidores y, en el caso del sector de las Telecomunicaciones, a instaladores. Por este motivo, dentro del mercado electrónico, es uno de los interlocutores cualificados ante la Administración española y comunitaria, y ante el resto de las instituciones y organismos de carácter público o privado.

La actividad de la ASIMELEC en relación con la seguridad de la información se desarrolla dentro de la Comisión para la Confianza y la Seguridad en las Tecnologías de la Información, creada con el objetivo de comunicar claramente la realidad actual del sector, a partir del importante desarrollo y crecimiento de este, para promocionar y concienciar sobre la necesidad de seguridad entre los usuarios.

La ASIMELEC ha hecho importantes contribuciones en el ámbito de la concienciación de la seguridad, entre las que se pueden mencionar el proyecto FARO (<http://faro.asimelec.se>), que consiste en una recopilación sobre los aspectos y las ideas en relación con la confianza en la sociedad de la información, o EXPOSEC (<http://exposec.asimelec.se>), una campaña informativa y demostrativa para las empresas españolas, y en especial para las pymes, sobre los mecanismos de seguridad existentes en el ámbito de las tecnologías de la información.

4.8_Agencia Catalana de Certificación (CATCert)

La CATCert es la entidad de certificación digital de las administraciones públicas catalanas. Tiene el objetivo de proporcionar a las administraciones catalanas los instrumentos necesarios para garantizar la seguridad de los trámites realizados efectuados mediante Internet.

Los servicio de seguridad de la CATCert incluyen la emisión de certificados digitales de varios tipos, orientados a los trabajadores de las administraciones públicas y a los ciudadanos (certificado idCAT), así como la prestación de servicios de creación y validación de firma, gestión de identidades y capacidades y archivo seguro, entre otros.

Las políticas públicas en materia de seguridad en la sociedad de la información

Ignacio Alamillo
Director de Asesoramiento e Investigación de la Agencia Catalana de Certificación (CATCert)

1_INTRODUCCIÓN

En este capítulo presentamos las principales políticas públicas y estrategias normativas en relación con la seguridad de los sistemas y redes de información.

Es indudable la existencia e importancia de la actuación pública, nacional e internacional, en esta materia, hasta el punto de que, como indica un importante estudio comparativo elaborado por la OCDE recientemente, los grandes elementos impulsores de la seguridad son la administración electrónica, la protección de las infraestructuras críticas y, más indirectamente, la protección de los datos personales.

Otra línea ampliamente considerada es la cooperación internacional, mediante grupos internacionales de intercambio de experiencias, en especial en las áreas de lucha contra la cibercriminalidad y en el establecimiento de equipos de respuesta a emergencias informáticas.

En general, se puede considerar que la mayoría de estados se encuentran en el proceso de establecer una aproximación basada en múltiples participantes –a demás de los gobiernos mismos– y una estructura de gobierno de alto nivel para implementar políticas de alcance nacional.

En este sentido, estos estados han hecho importantes avances en el desarrollo de marcos nacionales de políticas de seguridad, han aprobado medidas para combatir el cibercrimen y han establecido equipos de respuesta a incidencias de seguridad informática.

La administración electrónica como impulsora de la seguridad

Muchas administraciones públicas están implantando aplicaciones y servicios electrónicos para mejorar la eficiencia y la eficacia de sus actuaciones y ofrecer mejores servicios a la ciudadanía y al sector privado. Uno de los factores comunes en estas iniciativas de administración

electrónica es que afrontan la seguridad desde una perspectiva global, no únicamente tecnológica, sino incluyendo cuestiones como la prevención y la gestión del riesgo o la concienciación de los usuarios.

Hay que indicar en este punto que el beneficioso impacto de las actividades de administración electrónica abarca cada vez más al sector privado, puesto que la administración electrónica actúa como herramienta de difusión de la cultura de seguridad de la información. Por ejemplo, algunos estados obligan a las compañías o a los ciudadanos que se quieran conectar a la administración electrónica a adoptar medidas propias de seguridad. Como resultado, el sector privado recibe guías, mejores prácticas y documentación sobre seguridad de la información, y tiene la oportunidad de participar en conferencias y talleres específicos sobre concienciación y educación sobre seguridad.

En este capítulo veremos parte del impacto que comporta la administración electrónica en la adopción de la seguridad, aunque será en el tercer capítulo cuando abordaremos el análisis completo de esta cuestión, muy centrada, entre otros aspectos, en la identidad y las capacidades, la firma electrónica y otras fórmulas de garantía de la integridad y la autenticidad documental y, finalmente, en la conservación y el archivo en condiciones de seguridad de los documentos, expedientes, libros y registros de las administraciones públicas.

La protección de las infraestructuras críticas nacionales de información

Otra área de especial impacto en la implementación de políticas de seguridad de la información es la protección de las infraestructuras críticas de información, en las que confían los gobiernos, la industria, los ciudadanos y el resto de la sociedad (como por ejemplo, la energía, el suministro de agua, el transporte, el sector financiero, las telecomunicaciones y la salud).

La necesidad de impedir cualquier interrupción en la operación de estas infraestructuras lleva a los gobiernos a desarrollar políticas de seguridad dirigidas a los propietarios de estas infraestructuras. En algunos estados se han establecido diálogos entre gobierno e industria, basados en la colaboración publico-privada o en el intercambio de mejores prácticas e información sobre la complejidad técnica, de gestión y de personal relativa a la seguridad.

La protección de datos personales

En varios estados se constata que la aplicación de la legislación existente sobre protección de los datos de carácter personal actúa como impulsor indirecto en la aparición de una cultura de seguridad, sobre todo dado que la necesidad de proteger los datos personales es muy importante para el éxito de las iniciativas de administración electrónica dirigidas a la ciudadanía.

Por otro lado, la implementación de una normativa de seguridad se considera una de las formas más relevantes de demostrar el cumplimiento de esta legislación de protección de datos personales, por parte de entidades tanto privadas como públicas.

2_LAS POLÍTICAS PÚBLICAS GENÉRICAS DE IMPULSO DE LA SEGURIDAD DE LA INFORMACIÓN

En esta sección presentamos las políticas públicas de seguridad de la información, desde una perspectiva genérica, común a todo el problema de la seguridad de la información.

2.1_Estrategia global de seguridad de la información

El desarrollo de una estrategia global de seguridad de la información en el ámbito nacional empieza a ser una constante entre los estados, política habitualmente centrada en la necesidad de desarrollar herramientas de investigación y concienciación del público en cuanto al número cada vez más importante de amenazas y vulnerabilidades de la seguridad en línea.

En algunos casos, se han desarrollado políticas nacionales para coordinar actuaciones previas individuales que perseguían objetivos muy concretos, tratando de crear una política o una estrategia global de seguridad, mientras que en otros casos las políticas nacionales se han dirigido a implementar políticas de administración electrónica o, incluso, iniciativas singulares como las firmas electrónicas o las tarjetas de ciudadanos.

La mayoría de estados están en fase de establecer algún tipo de estrategia global de la seguridad de la información. Se caracterizan por:

- Una aproximación multidisciplinar y con múltiples participantes.
- Una estructura de gobierno de alto nivel.

Con respecto a la aproximación multidisciplinar y con múltiples participantes de las políticas nacionales de seguridad de la información, es interesante la manera en que la mayoría de iniciativas constatan que la cultura de la seguridad no aparece sencillamente a partir de las soluciones tecnológicas.

Por el contrario, hace falta una aproximación más amplia, que considere también los aspectos socioeconómicos y legales, hecho que otorga una dimensión multidisciplinar a las políticas.

Además, se considera que los gobiernos solos no pueden gestionar todos los retos y las cuestiones de seguridad. Esto implica una necesidad de involucrar al sector privado y a la sociedad civil, efecto que se puede conseguir con diferentes instrumentos, como las asociaciones publico-privadas, el desarrollo de mejores prácticas, el suministro de consejos y la participación en órganos comunes.

También es frecuente que los gobiernos recurran al sector privado para recibir consultoría sobre desarrollos tecnológicos y de implementación global. Algunos estados contratan universidades y expertos independientes para que les ayuden en cuestiones de política o generan la justificación necesaria para implementar una política concreta.

Como punto pendiente en la mayoría de estados, podemos encontrar la limitada participación de la sociedad civil en las cuestiones de seguridad de la información, hecho que indica la necesidad de mejorar la participación.

Con respecto a la estructura de gobierno de alto nivel, la mayoría de estados posicionan su estructura de gobierno de la seguridad en el nivel más alto. En muchas ocasiones, encontramos una dependencia de esta estructura de seguridad de la oficina del gobierno o del primer ministro, y de forma más escasa, como parece ser el caso del Estado español, esta responsabilidad está repartida entre diferentes departamentos ministeriales.

En todos los casos hay que indicar que una aproximación jerárquica, de arriba abajo, no resulta suficiente, sino que es necesaria la cooperación próxima de la industria y de todos los actores de la sociedad de la información, con el gobierno como coordinador de los esfuerzos y las actividades requeridas.

Más allá de las fronteras nacionales, hay que colaborar con las organizaciones internacionales y el resto de gobiernos para conseguir el objetivo

de la seguridad, dado que la actividad individual de los estados no puede dar respuesta al reto global de la seguridad de Internet, que no conoce fronteras.

En el Estado español, el Plan Avanza, liderado por el Ministerio de Industria, Turismo y Comercio, a través de la Secretaría del Estado de Telecomunicaciones y Sociedad de la Información, es uno de los instrumentos importantes respecto a la estrategia global española de seguridad de la información.

El Plan se estructura en cinco grandes áreas de actuación, una de las cuales se denomina «Nuevo contexto digital», que, en cuanto a la línea de seguridad y confianza (*e-Confianza*) se refiere, tiene los objetivos siguientes:

- Aumentar el grado de concienciación, formación y sensibilización de la ciudadanía, empresas y administraciones públicas en materia de seguridad de las TIC. De esta forma, se pretende reducir el número de empresas de más de 10 trabajadores con acceso a Internet que tienen problemas de seguridad, y situarlo en el 10% el 2010, y aumentar el número de particulares que toman precauciones de seguridad; concretamente, en 2010 el 60% de particulares habrá instalado un programa antivirus.
- Impulsar la identidad digital, considerando que en 2010 el 100% de los ciudadanos con DNI dispondrá de un identificador único, eficaz y práctico que se podrá utilizar intensivamente en todos los ámbitos.
- Estimular la incorporación de la seguridad en las organizaciones como factor crítico para el incremento de su competitividad, desarrollando las infraestructuras de seguridad necesarias y promoviendo la adopción de mejores prácticas, en especial, la certificación de la seguridad de la información. En 2010, el 95% de las empresas de más de 10 trabajadores habrá aplicado precauciones de seguridad.
- Desarrollar una infraestructura eficaz para la ejecución de la política nacional de seguridad de la información, coordinando los diferentes agentes y actuaciones, realizando una monitorización continuada del estado de la seguridad de la información y coordinando la representación internacional en materia de seguridad de las TIC.

Las medidas previstas por el Plan Avanza para conseguir estos objetivos son las siguientes:

Acciones iniciadas en 2006:

- **Medida SEG.01.** Difusión, comunicación y divulgación: campañas de sensibilización de gran público y jornadas sectoriales para administraciones públicas y pymes. Creación de plataformas para la protección del menor en Internet, protección contra el correo basura y contra los fraudes en Internet.
- **Medida SEG.04.** Desarrollo de una red de centros de seguridad: creación de centros de seguridad y establecimiento de los procedimientos y protocolos que permitan coordinar sus funciones y actuaciones. Creación de un CERT para la Administración, un CERT para las pymes y una unidad de lucha contra la violación de la privacidad (correo basura, pesca [*phishing*] y otros fraudes).
- **Medida SEG.06.** Impulso para la implantación de la identidad digital y la firma electrónica: potenciar el uso de la identidad digital y de la firma electrónica por parte de los diferentes segmentos de usuarios aprovechando especialmente la oportunidad que proporciona el DNI electrónico como infraestructura básica de seguridad.
- **Medida SEG.08.** Extensión de las mejores prácticas asociadas a la seguridad y la autorregulación: potenciar mejores prácticas en la industria y, en especial, en sectores críticos y administraciones públicas. Desarrollo de esquemas de autorregulación, especialmente para la lucha contra el correo basura y para la protección de los menores.
- **Medida SEG.09/10.** Actuaciones para la seguridad de la información y la confianza: crear una comisión para la seguridad de la información, con participación de los ministerios y las administraciones públicas competentes en materia de seguridad de la información, así como del sector privado. Desarrollar tareas de coordinación entre los diversos agentes, impulsando mecanismos de cooperación nacional e internacional, creando espacios de discusión y divulgando y entendiendo mejores prácticas en materia de seguridad de la información. Desarrollar medidas y metodologías para evaluar los indicadores de confianza electrónica con la elaboración de estudios sobre los adelantos en materia de uso de las tecnologías de seguridad por parte de los diferentes segmentos de usuarios (ciudadanos, empresas, hogares, etc.).

Acciones para el período 2007-2010:

- **Medida SEG.05** Promoción e impulso al desarrollo y la innovación de

tecnologías de seguridad: identificar necesidades y requisitos en materia de seguridad de los diferentes usuarios, trasladar a las empresas del sector de las TIC las necesidades mencionadas y crear redes de apoyo a la innovación en tecnologías de seguridad.

- **Medida SEG.07.** Promoción de la certificación de la seguridad, productos, servicios y procesos: potenciar y promocionar la evaluación y certificación de la seguridad de las TIC, principalmente mediante el desarrollo y la utilización de un esquema nacional de evaluación y certificación en el ámbito público y privado. Promover además su reconocimiento y la acreditación internacional.

Por otro lado, en este momento hay que trata la importante política de seguridad de la información del Ministerio de Administraciones Públicas y del Consejo Superior de Administración Electrónica, en colaboración con las comunidades autónomas, especialmente en los aspectos de gestión de la identidad y la seguridad del procedimiento administrativo, que analizaremos en otro capítulo.

También hay que hacer referencia a la actuación del CNI/CCN, dependiente del Ministerio de Defensa, en relación con la política de seguridad de información clasificada en el ámbito de la defensa y la seguridad nacional, incluyendo la participación en la OTAN, y la operación del esquema nacional de evaluación y certificación de la seguridad de la información, orientado a la seguridad de los productos, tanto de ámbito militar como civil, y que se presenta posteriormente, en este mismo capítulo.

Por lo tanto, podemos situar en estos tres departamentos (Ministerio de Industria, Turismo y Comercio, Ministerio de Administraciones Públicas y Ministerio de Defensa) la dirección actual y la coordinación de la política de seguridad de la información en el Estado español. Asimismo, hay que indicar la tarea de los cuerpos y las fuerzas de seguridad del Estado, incluyendo las policías autonómicas, en la lucha contra la cibercriminalidad y para lograr un uso más seguro de Internet.

2.2_Concienciación y formación sobre la seguridad de la información

Una de las políticas públicas genérica más importante es la que se orienta a incrementar los niveles de conciencia sobre la necesidad de la seguridad de la información, que la OCDE denomina la *cultura de la seguridad.*

Las Directrices de la OCDE para la seguridad de sistemas y redes de información: hacia una cultura de la seguridad del año 2002, que sustituyen a las Directrices de seguridad de los sistemas da información del año 1992, se han dedicado a este aspecto.

Las Directrices parten de la noción de un importante cambio en la informática, que ha pasado de sistemas aislados y redes privadas a un entorno basado en ordenadores personales, tecnologías convergentes, el uso masivo de redes públicas como Internet, y la interconexión de sistemas abiertos. En este nuevo contexto, Internet se ha convertido en parte de las infraestructuras operativas de sectores estratégicos como la energía, los transportes y las finanzas, y forma parte de la base del comercio y el gobierno electrónicos, además de permitir nuevas posibilidades a los ciudadanos.

Como contrapartida, han surgido nuevas vulnerabilidades y amenazas en la seguridad de la información y las comunicaciones, que hay que tratar adecuadamente. Por eso hay que empezar por un nivel suficiente de conocimiento de los nuevos retos de seguridad, para llegar a una cultura de la seguridad que abarque a todos los participantes en la sociedad de la información.

Los propósitos de las Directrices son los siguientes:

- Promover una cultura de seguridad entre todos los participantes como medio para proteger los sistemas y las redes de información.
- Incrementar la concienciación sobre el riesgo de los sistemas y redes de información; sobre las políticas, prácticas, medidas y procedimientos disponibles para poder hacer frente a estos riesgos, y sobre la necesidad de adoptarlos y ejecutarlos.
- Promover entre todos los participantes una mayor confianza en los sistemas y redes de información y en su forma de operación y de uso.
- Crear un marco general de referencia que ayude a los participantes a comprender los aspectos de seguridad y respeto a los valores éticos en el desarrollo y la ejecución de políticas coherentes, así como de prácticas, medidas y procedimientos para la seguridad de sistemas y redes de información.
- Promover entre todos los participantes, cuando sea posible, la cooperación y el intercambio de información sobre el desarrollo y la ejecución de políticas de seguridad, así como de prácticas, medidas y procedimientos.

- Promover el conocimiento en materia de seguridad como un objetivo importante que hay que lograr entre todos los participantes involucrados en el desarrollo y la ejecución de normas técnicas.

En el marco de estos objetivos generales, se proponen nueve principios, complementarios entre sí, de interés político y técnico, con indicación expresa de que los esfuerzos para fortalecer la seguridad de los sistemas y las redes de información deben respetar los valores democráticos, y en particular garantizar flujos de comunicación libres y abiertos, y la protección de los datos de carácter personal. Son los siguientes:

1. **Concienciación.** Los participantes deben ser conscientes de la necesidad de disponer de sistemas y redes de información seguros, y tener conocimiento de los medios para aumentar la seguridad.
2. **Responsabilidad.** Todos los participantes son responsables de la seguridad de los sistemas y las redes de información.
3. **Respuesta.** Los participantes han de actuar de manera adecuada y conjunta para prevenir, detectar y responder a incidentes que afecten la seguridad.
4. **Ética.** Los participantes deben respetar los intereses legítimos de terceros.
5. **Democracia.** La seguridad de los sistemas y las redes de información debe ser compatible con los valores esenciales de una sociedad democrática.
6. **Evaluación del riesgo.** Los participantes deben llevar a cabo evaluaciones de riesgo.
7. **Diseño y realización de la seguridad.** Los participantes han de incorporar la seguridad como un elemento esencial de los sistemas y las redes de información.
8. **Gestión de la seguridad.** Los participantes han de adoptar una visión integral de la administración de la seguridad.
9. **Evaluación continuada.** Los participantes deben revisar y evaluar periódicamente la seguridad de sus sistemas y sus redes de información, y llevar a cabo las modificaciones pertinentes sobre sus políticas, prácticas, medidas y procedimientos de seguridad.

Continuando en su actividad de promoción de la cultura la seguridad, la OCDE preparó en 2003 un plan de implementación, que identifica aspectos importantes sobre los diferentes roles o papeles de los participantes, teniendo en cuenta la necesidad de una cooperación continuada entre los gobiernos, las empresas y la sociedad civil.

En opinión de la OCDE, los gobiernos tienen la responsabilidad de emprender el liderazgo del desarrollo de la cultura de la seguridad, mediante los diversos roles que cumplen en relación con los sistemas y las redes de la información (desarrollador de políticas públicas, propietario y operador de sistemas y redes).

Durante el proceso de desarrollo de políticas públicas, los gobiernos deben promover la seguridad de las redes y los sistemas de información para generar confianza en su uso y asegurar mejor la seguridad global. Aunque se trata un proceso propio, los gobiernos deberían desarrollar estas políticas públicas de manera transparente, mediante consultas con otros gobiernos y con otros posibles interesados.

Los gobiernos deben desarrollar políticas públicas nacionales o regionales sobre seguridad de la información y garantizar la cooperación internacional para promover esta cultura global de la seguridad, mediante instrumentos como los siguientes:

- Medidas legales y técnicas para combatir la ciberdelincuencia, consistentes en la Convención del Consejo de Europa, que presentaremos posteriormente.
- Equipos y recursos personales altamente cualificados para apoyar la lucha coordinada contra el fraude informático.
- Instituciones preparadas para responder a ataques y emergencias informáticas y para intercambiar información relacionada con este tema, como por ejemplo los denominados CERT.
- Mecanismos de cooperación con el sector privado para combatir con más efectividad los problemas de seguridad.
- Apoyo a I+D en el campo de la seguridad de las tecnologías de la información.
- Actividades de concienciación pública, formación y educación del público.
- Suministro de recursos de información al público sobre la seguridad de los sistemas y las redes de información.

Como propietarios y operadores de sistemas y redes de información, los gobiernos comparten rol con las empresas, otras organizaciones y los individuos en relación con el aseguramiento del uso correcto de los sistemas y las redes, dentro de la cultura de la seguridad.

En general, dado el volumen de los sistemas de los gobiernos con relación al territorio nacional, deberían ser un modelo de operación segura para guiar al resto de organizaciones y ciudadanos, mediante el establecimiento de mejores prácticas y otras técnicas de mejora organizativa; mientras que, en particular, hace falta considerar la capacidad de adquisición de tecnología que tienen los gobiernos como un mecanismo para influir en la mejora de la seguridad de los productos ofrecidos al mercado.

El análisis realizado por la OCDE a finales de 2004 sobre las actividades gubernamentales en relación con la seguridad de la información y, en particular, sobre el marco normativo en apoyo de la seguridad, ha mostrado que un grupo importante de estados identifica la firma electrónica y la certificación digital como aspecto esencial de su estrategia legal en apoyo de la seguridad.

Adicionalmente, se identifican como elementos importantes la protección de datos personales y las medidas de inspección y de control sobre las comunicaciones electrónicas.

Con respecto a los programas de sensibilización sobre la seguridad de la información, la ENISA (Agencia Europea de Seguridad de las Redes y de la Información) ha publicado un interesante documento, dirigido a ayudar a los estados miembro de la Unión Europea a preparar este tipo de programa, donde expone los principales beneficios:

1. Representar un punto de referencia y un motor para una serie de actividades de sensibilización, formación y educación relacionadas con la seguridad de la información, algunas de las cuales ya pueden existir, pero posiblemente necesiten ser objeto de una mayor coordinación y optimización.

2. Transmitir las directrices o prácticas recomendadas importantes que sean necesarias para proteger los recursos de información.

3. Facilitar información general y específica sobre los riesgos y controles de la seguridad de la información a las personas que la hayan de conocer.

4. Informar a las personas de sus responsabilidades en relación con la seguridad de la información.

5. Estimular a las personas a adoptar las directrices o prácticas recomendadas.

6. Crear una cultura de seguridad más arraigada, con una comprensión y un compromiso de amplio alcance con la seguridad de la información.

7. Contribuir a potenciar la coherencia y la eficacia de los controles de la seguridad de la información y fomentar la adopción de controles eficaces respecto a su coste.

8. Contribuir a reducir el número y el alcance de las infracciones de la seguridad, y disminuir así el coste directamente (por ejemplo, daños producidos por virus) e indirectamente (por ejemplo, reducción de la necesidad de investigar y solucionar las infracciones). Estas son las principales ventajas financieras del programa.

Los últimos estudios muestran que los estados ya están activamente involucrados en iniciativas para incrementar la concienciación pública en relación con la cultura de la seguridad, iniciativas que incluyen presentaciones públicas y la distribución de materiales informativos.

Por ejemplo, en el Estado español se pueden mencionar varias iniciativas en este sentido, incluyendo el proyecto de divulgación del estado de la seguridad FARO, de ASIMELEC, la campaña itinerante EXPOSEC para presentar aspectos de seguridad, también organizada por ASIMELEC en colaboración con el Ministerio de Industria, Turismo y Comercio, la constante tarea divulgadora de las cámaras de comercio, en particular mediante Camerfirma, o la actuación de la sociedad civil, por ejemplo, mediante el Foro de las evidencias electrónicas, que genera discusión en línea y reuniones periódicas con todos los actores relacionados con aspectos relativos a la seguridad de la información, como la generación de pruebas electrónicas con reconocimiento judicial.

Los actos públicos tratan una importante diversidad de temas de seguridad, cuestiones muy generales o más específicas como la gestión de riesgos, la autenticación electrónica, las firmas electrónicas o las PKI. El público destinatario de estos acontecimientos también es variable, desde el público en general hasta expertos que trabajan en los sectores privado y público. En particular, muchos gobiernos organizan de forma regular ac-

tos internos para formar a su personal (por ejemplo, el CCN tiene una importante actividad en este sentido), con una incipiente tendencia a abrir estos actos al sector privado y a la ciudadanía, dado que puede ser una manera de llegar a estos destinatarios de forma más efectiva.

Por otro lado, la preparación y distribución gratuita de recomendaciones, mejores prácticas y guías generales es una manera muy importante de vehicular las políticas de concienciación de la seguridad.

Además, en varios estados existe la tendencia de redactar mejores prácticas y guías en cuestiones técnicas y operativas como la autenticación en línea, las firmas electrónicas, las redes inalámbricas, las redes de igual a igual, la gestión del riesgo y la respuesta a incidentes.

2.3_Análisis y gestión de riesgos

El análisis y la gestión de riesgos también es una política genérica importante en varios estados, incluyendo el español.

Las iniciativas en relación con el análisis y la gestión de riesgos incluyen casos como el desarrollo de metodologías (Francia, con EBIOS, o España, con MAGERIT), o normas y guías (Noruega, Japón o los Estados Unidos). Algunas iniciativas se completan con una red específica de usuarios, como sucede en Francia, para el intercambio de información y para continuar el desarrollo de la metodología.

Otras iniciativas incluyen la creación y el suministro de herramientas automáticas para asistir en la realización de los análisis de riesgo, como es el caso de la herramienta PILAR del CCN o de las herramientas del método CRAMM británico.

Hay que indicar que el uso de las técnicas y herramientas de análisis y gestión de riesgo no está limitado a las tecnologías de la información, sino que se empieza a utilizar en áreas como los desastres naturales, el sector de las telecomunicaciones y, de forma más genérica, para proteger las infraestructuras críticas.

Asimismo, en algunos estados, como Austria, el análisis de riesgos forma parte de los procesos de supervisión y control de los prestadores de servicios de certificación de firma electrónica, mientras que en Finlandia se ha utilizado como herramienta para los proyectos de cooperación financiera liderados por el gobierno.

2.4_Evaluación de la seguridad de la información en productos y servicios

Con una orientación más particular a los productos, ya está consolidada la política de los estados de fomentar la calidad y la seguridad de los productos mediante su certificación de acuerdo con metodologías formales. Cada vez son más los estados que exigen certificaciones de seguridad a los productos que han de adquirir para desarrollar sus tareas.

La forma de implementar esta evaluación y certificación de la seguridad de la información es la creación de un esquema nacional de evaluación, que la organización sistemática de las funciones de evaluación y certificación de la seguridad en un país concreto, bajo la autoridad de un consejo de dirección o una entidad de certificación de la seguridad, con el objetivo de asegurar que se mantienen unos altos niveles de competencia y de imparcialidad y que se consigue la coherencia global del sistema.

Los esquemas nacionales se crean al amparo del Acuerdo de reconocimiento mutuo sobre los certificados de evaluación de la seguridad de las tecnologías de la información, del 26 de noviembre de 1997, aprobado por el grupo de altos funcionarios en seguridad de los sistemas de información de la Comisión Europea, de acuerdo con el mandato contenido en el punto tercero de la Recomendación del Consejo 95/144/CE, de 7 de abril de 1995.

Inicialmente centrados en la certificación de productos de acuerdo con los criterios de evaluación de la seguridad de las tecnologías de la información (ITSEC) de 1991, actualmente los estados signatarios del Acuerdo también han acogido los ITSEC (Common Criteria o CC, ISO 15408), mediante la modificación del Acuerdo de 1997, así como la firma del Acuerdo sobre el reconocimiento de los certificados de criterios comunes en el campo de la seguridad de la tecnología de la información, de 23 de mayo de 2000.

Los esquemas nacionales de evaluación y certificación de la seguridad de las tecnologías de la información funcionan de la siguiente manera:

- El esquema nacional está dirigido por un único organismo de certificación, de acuerdo con una política establecida por el organismo de certificación mismo o por un consejo de dirección del esquema nacional, que debe crear y hacer cumplir los reglamentos operativos del esquema nacional.

- El organismo de certificación debe ser un organismo independiente, declarado competente por una norma legal o administrativa, o bien acreditado por una entidad de acreditación nacional. En cualquier caso, debe cumplir los requisitos EN 45011 o Guía ISO 65 o los requisitos descritos en el anexo C del Acuerdo ITSEC.
- El organismo autoriza la participación de los servicios de evaluación del esquema, controla su funcionamiento y actividad de evaluación, examina todos los informas de evaluación, elabora un informe de certificación respecto a cada evaluación y publica los certificados y los informes de certificación, así como una lista de productos certificados.
- El servicio o laboratorio de evaluación, además de estar autorizado por el organismo de certificación, debe estar previamente acreditado por una entidad de acreditación nacional, excepto si ha sido creado y declarado competente por una norma legal o administrativa. En cualquier caso, debe cumplir los requisitos EN 45001 o Guía ISO 25.

El CCN, creado por el Real decreto 421/2004, ha sido nombrado el órgano competente de certificación del esquema nacional de evaluación y certificación de la seguridad de las tecnologías de la información; el Instituto Nacional de Técnica Aeroespacial (INTA) actúa como laboratorio de evaluación autorizado para productos que traten información clasificada y no clasificada; la empresa APPLUS actúa como laboratorio de evaluación autorizado para productos que traten información no clasificada, y la ENAC como entidad de acreditación.

2.5_Investigación y desarrollo en seguridad de la información

I+D en materia de seguridad de la información es una de las políticas más habituales de los estados adelantados en la cultura de la seguridad, especialmente por el impacto posterior en la competitividad de las empresas productoras de tecnologías de seguridad, que comercializan sus productos en el mercado global.

En este sentido, desde una perspectiva de política de la UE, la Resolución del Consejo de 22 de marzo de 2007, sobre una estrategia para una sociedad de la información segura en Europa, considera que los recursos destinados a I+D+I, tanto en el ámbito nacional como comunitario, constituyen uno de los elementos fundamentales para reforzar el nivel de seguridad de las redes y de la información de los nuevos sistemas, aplicaciones y servicios.

En consecuencia, se considera importante intensificar el esfuerzo a nivel europeo en los ámbitos de la búsqueda y la innovación en relación con la seguridad, en particular mediante el Séptimo programa marco y el Programa marco para la competitividad y la innovación.

Adicionalmente, hay que esforzarse para implantar medidas destinadas a difundir y promover la explotación comercial de los resultados, incluyendo la evaluación de su utilidad para la comunidad en su conjunto, hecho que contribuirá a mejorar la capacidad de los proveedores europeos para suministrar soluciones de seguridad que respondan a las necesidades específicas del mercado europeo.

La mayoría de estados reconocen la importancia de las actividades de I+D para la seguridad de la información, puesto que son la clave para producir soluciones innovadoras que puedan hacer frente a sus requisitos presentes y futuros. Como se ha adelantado, la inversión en I+D en seguridad de la información se percibe como un elemento que contribuye al incremento global de innovación y competitividad de los estados.

Aun así, los estudios muestran que pocos estados han establecido programas específicos de investigación en seguridad de la información con fondos públicos, mientras que la mayoría de estados financian la investigación en seguridad dentro de programas más amplios de investigación, habitualmente relativos a los aspectos informáticos (por ejemplo, criptografía) y tecnológicos, sin que se consideren los aspectos sociales, legales y económicos de la seguridad de la información.

En general, estas tareas de I+D las desarrollan las universidades, habitualmente institutos creados específicamente para tratar la cuestión de la seguridad de la información y, con menos frecuencia, en cooperación con la industria. También es notable que la cooperación internacional en I+D de la seguridad de la información es limitada.

Como ejemplos de las actividades en esta área, se pueden mencionar las siguientes:

- El proyecto de los Países Bajos SENTINEL, cuyo objetivo es desarrollar aplicaciones seguras para sistemas de usuario, administración electrónica y comercio electrónico, presenta una interesante aproximación multidisciplinar.
- El proyecto Oppidum (Francia) y el IKT SoS (Noruega).

- El proyecto Seguridad 2020 (España) y los proyectos españoles de investigación específica, dentro de líneas de alcance tecnológico más amplio (caso similar en Austria, Dinamarca, Alemania, Corea, el Reino Unido o los Estados Unidos).

En algunos casos, las tareas de investigación las llevan a cabo organizaciones gubernamentales con responsabilidades de seguridad de la información, como la oficina federal alemana de seguridad de la información, la agencia coreana de seguridad de la información, el establecimiento público canadiense de seguridad de las comunicaciones o la división de ciberseguridad del departamento de interior de los Estados Unidos. Estas tareas de búsqueda persiguen el desarrollo de nuevas soluciones, como por ejemplo RFID (identificación por radiofrecuencia), biometría o tecnología inalámbrica, o solucionar necesidades o problemas inmediatos.

En otros casos, los estados facilitan la participación de la industria y de otras instituciones independientes de investigación en sus iniciativas de investigación en seguridad de la información, como es el caso de España, Alemania, los Países Bajos o Austria.

2.6_Normalización de la seguridad de la información

La normalización de la seguridad de la información se ha ido realizando en las denominadas *organizaciones de desarrollo de normas*, expresión que se refiere a los organismos legalmente designados para la normalización internacional (como por ejemplo, ISO/CEI, ITU-T, ETSI o CEN), y a otros organismos que producen especificaciones técnicas –a veces basadas en normas previas– que suelen ser normas de hecho (como por ejemplo, IETF u OASIS).

Teniendo en cuenta la aproximación de los diversos organismos de normalización –y de sus comités o grupos internos de trabajo– al problema de seguridad, que se produjo inicialmente alrededor de los problemas de seguridad de tecnologías concretas para pasar en un segundo momento a una visión más general de la seguridad, encontramos una ingente cantidad de normas y especificaciones técnicas.

La ITU-T ha elaborado un primer inventario parcial sobre el estado actual de la normalización de la seguridad realizada por la ITU-T, ISO/CEI, IEEE, ETSI, IETF y OASIS, actualizado en febrero de 2007, empleando la taxo-

nomía siguiente, que muestra el volumen de normas vigentes que hay que considerar:

- Guías generales sobre seguridad de la información y las comunicaciones: 26 normas/especificaciones.
- Marcos de trabajo, modelos y arquitecturas de seguridad: 35 normas/especificaciones.
- Documentos de normas de gestión y guía de gestión de seguridad: 16 normas/especificaciones.
- Políticas formales de seguridad y mecanismos de política: 1 norma/especificación.
- Asesoramiento y criterios de evaluación de seguridad: 12 normas/especificaciones.
- Requisitos de seguridad de línea base: 2 normas/especificaciones.
- Detección de intrusos: 3 normas/especificaciones.
- Servicios de seguridad:
  - Servicios genéricos de seguridad: 2 normas/especificaciones.
  - Servicios de control de acceso: 2 normas/especificaciones.
  - Servicios de autenticación: 8 normas/especificaciones.
  - Servicios de tercera parte de confianza: 1 norma/especificación.
  - Servicios de auditoría y alerta: 7 normas/especificaciones.
- Mecanismos de seguridad:
  - Mecanismos de autenticación: 23 normas/especificaciones.
    - Firma electrónica: 26 normas/especificaciones.
    - Targetas inteligentes: 13 normas/especificaciones.
  - Mecanismos de confidencialidad:
    - Técnicas y algoritmos de cifraje: 67 normas/especificaciones.
    - Gestión de claves: 19 normas/especificaciones.
    - Otros mecanismos criptográficos: 4 normas/especificaciones.
  - Mecanismos de integridad:
    - Sistemas de comprobación: 1 norma/especificación.
    - Sistemas de resumen: 5 normas/especificaciones.
  - Mecanismos de irrefutabilidad (*no-repudio*):

    - General: 3 normas/especificaciones.
    - Mecanismos de tercera parte de confianza: 1 norma/especificación.
    - Mecanismos de firma digital: 6 normas/especificaciones.
    - Sello de fecha y hora: 4 normas/especificaciones.
- Seguridad de red: 5 normas/especificaciones.
- Seguridad de la capa de transporte: 1 norma/especificación.
- Protocolos de seguridad: 53 normas/especificaciones.
- Mensajería segura: 24 normas/especificaciones.
- PKI y directorio: 52 normas/especificaciones.
- Recuperación de desastres: 1 norma/especificación.
- Redes de nueva generación (NGN): 8 normas/especificaciones.
- Terminología y glosarios de seguridad: 4 normas/especificaciones.
- Seguridad en sectores específicos:
  – Multimedia: 30 normas/especificaciones.
  – Seguridad de señales y servicios de televisión: 7 normas/especificaciones.
  – Facsímiles: 5 normas/especificaciones.
  – Móvil: 58 normas/especificaciones.
  – Satélite: 7 normas/especificaciones.
  – Miscelánea: 2 normas/especificaciones.

De este inventario, que hay que recordar que es parcial y sólo considera normas vigentes (ninguna de las versiones anteriores) y no contabiliza las normas idénticas o repetidas (por ejemplo, muchas de las recomendaciones ITU-T también han sido publicadas por el ISO/CEI), surge un cuerpo normativo básico de 544 normas y especificaciones, muchas de las cuales son complementarias entre sí, hecho que pone de manifiesto el ingente esfuerzo realizado para normalizar la seguridad.

A pesar de que parece que la tarea de normalización está completa, desde una perspectiva de política de la UE, la Resolución del Consejo, de 22 de marzo de 2007, sobre una estrategia para una sociedad de la información segura en Europa, indica que la normalización y la certificación de productos, servicios y sistemas de gestión, en particular los suministrados por instituciones existentes, debe recibir una atención especial,

como medio para difundir las buenas prácticas y la profesionalidad en el ámbito de la seguridad de las redes y de la información.

Por otro lado, se considera que la adopción, cuando proceda, de posibles nuevas normas abiertas e interoperables será beneficiosa para las nuevas tecnologías emergentes, como los dispositivos de identificación por radiofrecuencia y la televisión móvil. Se recomienda el impulso de las actividades de los organismos europeos de normalización en este ámbito.

3_ÁREAS DE ESPECIAL INTERÉS EN LA ACTUACIÓN PÚBLICA SOBRE SEGURIDAD DE LA INFORMACIÓN

En esta sección presentamos las principales áreas de actuación pública, en atención a materias específicas, excluyendo los aspectos de gestión de identidad y capacidades, protección de datos personales y firma electrónica, que se tratan de forma monográfica en el capítulo tercero de esta segunda parte.

3.1_Ciberdelincuencia

La sociedad de la información representa una oportunidad indudable de desarrollo humano, social y económico, pero su estructuración también permite la aparición de nuevas formas de criminalidad empleando la tecnología. Además, las consecuencias de los comportamientos delictivos pueden tener efectos de alcance superior dada la ausencia de limitaciones geográficas o fronteras nacionales, como demuestran los ataques a la propiedad intelectual o los virus informáticos; mientras que las medidas técnicas de protección de los sistemas de información deben ser implementadas de acuerdo con las medidas legales de prevención y lucha contra los delitos.

La ciberdelincuencia ha sido un reto para la normativa jurídica tradicional, precisamente por la internacionalidad intrínseca. Cada vez es más frecuente que los delincuentes actúen desde territorios diferentes de aquellos en los cuales se manifiestan y producen efectos los delitos, hecho que no encaja con las leyes nacionales tradicionales, que tienen una fuerte orientación territorial, de forma que es necesario tratar el problema desde el derecho internacional. Esto ha motivado instrumentos como el Convenio europeo 185 sobre cibercrimen, firmado en Budapest el 23 de noviembre de 2001, y su Protocolo adicional 189 sobre criminalización

de los actos de naturaleza racista y xenófoba cometidos mediante sistemas de información.

El Convenio tiene los objetivos principales siguientes: armonizar los aspectos de la ley sustantiva de los estados que sean relativos al área de cibercrimen; ofrecer un marco suficiente procedimental para perseguir los delitos mencionados, y establecer un régimen efectivo y rápido de cooperación internacional.

Las conductas delictivas o ciberdelitos cubiertos por el Convenio europeo son los siguientes: acceso ilícito, intercepción ilícita, interferencia de sistemas, abuso de los dispositivos y sistemas, falsificación informática, fraude informático, pornografía infantil y delitos contra la propiedad intelectual y derechos conexos.

Hoy se puede decir que la mayoría de estados han adaptado su marco jurídico para tratar el problema del cibercrimen, en mucho casos siguiendo el Convenio europeo y otros instrumentos legislativos de la UE.

En algunos casos se ha optado por establecer una función central o unidad de coordinación de las cuestiones de cibercrimen, organismos que colaboran con el sector privado y que participan en iniciativas de cooperación internacional para responder mejor a la naturaleza global del problema. Los órganos centrales de lucha contra el cibercrimen son, en algunos estados, complementados por unidades regionales o locales, y en algunos casos también por unidades privadas. En algunos estados, además, estas unidades también llevan a cabo tareas de divulgación en el sector privado, en particular para pymes, y para los ciudadanos.

En relación con la cooperación internacional, se pueden mencionar la red europea de institutos de ciencias forenses en criminalidad informática, la Interpol, la UE, el CoE y la Red 24/7 de criminalidad de alta tecnología. También es muy frecuente la colaboración a partir de acuerdos bilaterales entre los estados.

En el Estado español el Ministerio de Interior es referencia obligada en la lucha contra el cibercrimen, a través de las unidades de la Policía Nacional y la Guardia Civil, que disponen de unidades especializadas en esta materia, complementadas por unidades similares a algunas policías autonómicas, como por ejemplo los Mossos de Esquadra en Cataluña.

3.2_Centros de respuesta a incidentes de seguridad (CERT y CSIRT)

Actualmente, todos los estados disponen de un equipo o más de respuesta a emergencias informáticas (CERT) o equipos de respuesta a incidentes de seguridad (CSIRT), o están en fase de crearlos. Suelen ser instituciones tanto públicas como privadas, gubernamentales o universitarias. Como mínimo en dos estados, las actividades de estos organismos están complementadas por centros de asistencia e intercambio de información de seguridad (ISAC).

Estos centros facilitan compartir la información de seguridad dentro de un grupo de miembros que operan en sectores similares, con una fuerte orientación a la cooperación internacional. Esto permite un mejor intercambio de información y buenas prácticas. En este sentido, la mayoría de estados cooperan en el ámbito regional (por ejemplo, las redes europeas TF-CSIRT y EGC o APCERT) o global (FIRST).

Uno de los retos de futuro importantes para estos centros es la operación 24/7, que se está desarrollando en varios estados (Canadá, Finlandia).

En Japón y en los Estados Unidos se pueden encontrar ISAC específicos del sector de las telecomunicaciones para compartir información dentro de este sector, mientras que países como Canadá están desarrollando programas con ejercicios de respuesta a incidentes que involucran a los sectores privado y público.

Algunos estados operan sistemas de monitorización del tráfico de red para detectar determinadas amenazas a tiempo real, como Japón o Corea.

3.3_Comunicaciones comerciales no solicitadas (correo basura)

El correo basura ha incrementado considerablemente en los últimos cinco años, y representa entre el 50% y el 80% de todos los mensajes de correo electrónico que reciben los usuarios, con un coste superior a los 39.000 MEUR en 2005.

Considerado un negocio en sí mismo, que consiste en el alquiler o la venta de listas de correos electrónicos recolectados en la red para propósitos comerciales, el correo basura requiere una inversión mínima para enviar los elevados volúmenes de correos electrónicos, y devuelve muchas veces esta inversión. También es cierto que inversiones relativamente pequeñas pueden reducir de forma muy considerable el

problema, como es el caso de los Países Bajos, en el que la reducción del 85% del correo basura ha comportado un coste aproximado de 570.000 € en hardware y software.

El correo basura ha pasado de ser una práctica comercial, molesta para algunos pero esencialmente lícita, a ser cada vez instrumento de fraude y comisión de delitos, como es el caso de los mensajes de pesca, en que se suplanta la identidad de páginas web lícitas, como las páginas de las entidades financieras, con la intención de robar la identidad (y la contraseña) de los usuarios o perjudicar la reputación de las mencionadas entidades.

Por otro lado, sigue creciendo el uso del correo electrónico para la diseminación de software espía o de software de captura de comportamiento en línea de los usuarios. En muchos casos, este software espía puede obtener información personal muy sensible y divulgarla, como es el caso de números de tarjeta financiera.

El envío masivo de correos electrónicos también se produce por efecto de los virus y los gusanos, que toman el control de un ordenador infectado y lo convierten en un *botnet*, que esconde la identidad del pescador pirata y genera los envíos de los correos. Se estima que como mínimo el 50% de los correos fraudulentos provienen de estos sistemas, con un impacto global de unos 11.000 MEUR en 2005.

En la UE se adoptó una directiva sobre la privacidad y las comunicaciones electrónicas en 2002 que trata de limitar el correo electrónico mediante el principio del consentimiento para las comunicaciones comerciales en las personas físicas.

Posteriormente, en 2004 se preparó una Comunicación de la Comisión sobre correo basura en la cual se identifican actuaciones para complementar esta d, y se llama a la acción a los diversos actores en relación con la concienciación, la cooperación y la ejecución de las medidas legales oportunas para combatir este problema, mensaje que se encuentra también en la Comunicación de la Comisión sobre correo basura del 2006.

Las medidas propuestas en el ámbito comunitario han sido implementadas por la legislación española, tal y como se ha expuesto en la primera parte de este libro.

Respecto a las medidas adoptadas por la industria europea para luchar contra el correo basura, en cumplimiento de la Directiva 2002/58, el estudio elaborado por ENISA ofrece algunas recomendaciones importantes:

- Las medidas técnicas de los proveedores son muy variadas, y dependen del tipo de amenaza que trata de evitar cada proveedor y la naturaleza específica del segmento de negocio en que se encuentra. Se considera, sin embargo, que las medidas técnicas se podrían mejorar y se recomienda evaluar la posibilidad de solicitar a los proveedores que informen sobre las medidas técnicas de seguridad de sus servicios, e incentivar a los proveedores para que colaboren en la protección global de las redes, y no sólo de sus sistemas.
- En relación con las medidas organizativas de los proveedores, se considera posible y conveniente mejorar la guía que reciben actualmente, y enfatizar, por ejemplo, la recolección y diseminación de mejores prácticas, así como suministrar guías también a los ciudadanos sobre respuesta a incidentes de seguridad y mejorar la forma en que se suministra información sobre los contactos en los casos de violaciones de seguridad y abuso de correo electrónico.
- En relación con el envío de correo basura, el estudio subraya que los proveedores se preocupan menos por recibir correo basura, puesto que confían bastante en la regulación contractual con sus clientes, en la cual prohíben el envío de correos basura y se eximen de responsabilidad. Es necesario mejorar la concienciación de los proveedores sobre los efectos de este correo basura, para tratar de reducir el volumen de mensajes ilícitos generados desde la UE.
- Desde una perspectiva técnica, no hay una protección total contra el correo basura. Aunque la protección técnica contra el correo basura se mejore, sería una mejora marginal. Esto implica que, salvo que los modelos económicos del correo basura se modifiquen considerablemente, los proveedores pueden hacer poco más que aplicar una variedad de contramedidas.
- Se podría fomentar la reobligación de informar sobre los casos importantes de abuso de correo electrónico a la autoridad nacional competente, que en España es la Agencia Española de Protección de Datos, hecho que permitiría que estas autoridades pudieran tener un papel más activo.
- En relación con las diferentes posibilidades del consentimiento que se contienen en la normativa vigente, incluyendo el consentimiento previo o posterior, se considera recomendable aclarar los términos legales para evitar problemas interpretativos.

- Dada la variedad de los posibles métodos de identificación de los usuarios, sería muy recomendable trabajar los aspectos de normalización y de interoperabilidad de estos, como por ejemplo la autenticación del remitente.
- Una de las cuestiones importantes que requiere más guía es la consideración sobre el estado del arte y el coste de las implementaciones de seguridad. Se recomienda determinar y seguir las mejores prácticas de la industria a nivel europeo.
- Todos los proveedores deberían ser proactivos y controlar sus redes, e informar sobre las redes que vigilan.
- Es muy importante que los proveedores informen del riesgo de infracciones de seguridad para disponer de una visión general del riesgo real para cada problema particular. Todavía sería más efectiva una potencial obligación de informar de las infracciones efectivas de seguridad, de forma pública o anónima.
- Se tendría que aclarar y simplificar la relación entre las autoridades nacionales que controlan las comunicaciones electrónicas y las que controlan la transmisión de correos no solicitados. También es muy deseable la coordinación a escala del Estado miembro o de la UE.

3.4_Protección de la seguridad de les infraestructuras críticas de información y comunicaciones

Un área de actuación específica en materia de seguridad de la información es la protección de las infraestructuras críticas, que ha recibido una atención particular a raíz de los ataques terroristas de los últimos años. La política comunitaria en esta materia se puede ver en las Comunicaciones (2004) 702, (2005) 576 y en la propuesta de la directiva europea sobre identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar la protección, que presentamos a continuación.

Las consecuencias de un ataque contra los sistemas industriales de control de las infraestructuras críticas podrían ser muy diversas. Se considera que un ataque cibernético causaría pocas víctimas o ninguna, pero que podría implicar la pérdida de servicios de infraestructura vitales, como por ejemplo el servicio telefónico en que confían los servicios de emergencia, mientras que ataques contra los sistemas de control de infraestructuras químicas podrían implicar fugas de materiales tóxicos, que en este caso podrían producir víctimas mortales.

Por otro lado, hay que indicar que los efectos en cascada pueden ser muy dañinos, y provocar grandes caídas de los servicios públicos. El ciberterrorismo podría, además, amplificar los efectos de un ataque físico. Un ejemplo sería un ataque convencional contra un edificio, combinado con un corte temporal del servicio eléctrico o telefónico. Los atrasos en la respuesta de urgencias podrían aumentar el número de víctimas y el pánico de la población.

Las infraestructuras críticas son instalaciones, redes, servicios y equipamientos físicos y de tecnología de la información, cuya interrupción o destrucción tendría un impacto más grande en la salud, la seguridad o el bienestar económico de los ciudadanos o en un funcionamiento eficaz de los gobiernos de los estados miembro. Las infraestructuras críticas están presentes en numerosos sectores de la economía: actividades bancarias y financieras, transporte y distribución, energía, servicios, salud, suministro de alimentos, comunicaciones, PKI. Algunos elementos críticos de estos sectores no son infraestructuras en sentido estricto, sino que son redes o cadenas de suministro que contribuyen a la entrega de un producto o servicio esenciales.

Las siguientes infraestructuras se consideran críticas:

- Centrales y redes de energía (electricidad, producción de petróleo y gas, instalaciones de almacenamiento y refinerías, sistemas de transmisión y distribución).
- TIC (telecomunicaciones, sistemas de radiodifusión, programas informáticos, apoyo físico y redes, incluyendo Internet).
- Finanzas (banca, valores e inversión).
- Salud (hospitales, centros de atención sanitaria y de suministro de sangre, laboratorios y empresas farmacéuticas, búsqueda y rescate, servicios de urgencia).
- Alimentación (seguridad alimentaria, medios de producción, mayoristas, industria alimentaria).
- Agua (embalses, almacenamiento, tratamiento, redes).
- Transporte (aeropuertos, puertos, instalaciones intermodales, ferrocarril, redes de transporte público, sistemas de control de tránsito).
- Producción, almacenamiento y transporte de mercancías peligrosas (materiales químicos, biológicos, radiológicos y nucleares).

- Estado (servicios críticos, instalaciones, redes de información, activos, lugares y monumentos principales).

Estas infraestructuras pueden ser de propiedad o gestión tanto del sector público como del privado. Aun así, en la Comunicación 574/2001, de 10 de octubre de 2001, la Comisión ha declarado que la aplicación de determinadas medidas de seguridad por parte de los poderes públicos como consecuencia de los ataques dirigidos contra la sociedad en conjunto y no contra las empresas debe ser responsabilidad del Estado. El sector público tiene, por lo tanto, un papel fundamental.

En una visión más general, muchos estados están en proceso de establecer actividades para la protección de la infraestructura de información crítica (Japón, Noruega, los Estados Unidos), con planes de acción o estrategias que describen las responsabilidades, mejores prácticas y procedimientos en respuesta a varios tipos de incidentes. Estados como Australia, Canadá, Francia o Alemania están muy adelantados en el estudio o ya empiezan a aplicar medidas parecidas.

Respecto a la organización, se pueden encontrar fórmulas bien diferentes, como comités permanentes (Japón o Corea), grupos de trabajo (Alemania), consejos asesores (Australia), centros interdepartamentales (Reino Unido) o proyectos específicos (Países Bajos). Todos responden habitualmente a la necesidad de facilitar y fomentar el intercambio de información sobre la seguridad de las infraestructuras críticas dentro del sector público, y también con participación del sector privado (en pocos casos con participación de los ciudadanos). Aun cuando se trata generalmente de estructuras nacionales, en algunos casos hay medidas similares y complementarias en el ámbito regional y en sectores específicos.

La cooperación entre los gobiernos y el sector privado es frecuente, puesto que, como se ha indicado, la parte más importante de esta infraestructura es propiedad o es operada por entidades privadas (hasta el 85% en los Estados Unidos, por ejemplo). Algunos estados han establecido unidades de coordinación en el sector público, parecidas a las que ya había para la coordinación de la seguridad de la información.

Algunos estados están en proceso de establecer medidas legales para la protección de las infraestructuras críticas, como Francia o España en relación con la legislación sectorial de las telecomunicaciones, o Finlandia, que dispone de una instrucción específica del Ministerio de Finanzas que regula la seguridad de los sistemas de información crítica.

Desde una perspectiva de la política de la UE, como se ha presentado anteriormente, el CoE de junio de 2004 instó a la Comisión a elaborar una estrategia global sobre protección de infraestructuras críticas. El 20 de octubre de 2004, la Comisión adoptó la Comunicación sobre protección de las infraestructuras críticas en la lucha contra el terrorismo, con propuestas para mejorar la prevención, la preparación y la respuesta de Europa ante atentados terroristas que afecten a las infraestructuras críticas.

En las conclusiones del CoE sobre prevención, preparación y respuesta a los ataques terroristas y en el Programa de solidaridad de la UE sobre las consecuencias de las amenazas y ataques terroristas, adoptado por el CoE en diciembre de 2004, se da soporte al propósito de la Comisión de iniciar un programa europeo de protección de las infraestructuras críticas (PEPIC) y se aprueba la creación por parte de la Comisión de una red de información sobre alertas en infraestructuras críticas (CIWIN).

En noviembre de 2005, la Comisión aprobó el Libro verde sobre un PEPIC, que expone las posibilidades de acción de la Comisión para crear el PEPIC y la CIWIN, actuaciones previas que han conducido a preparar una propuesta de Directiva (2006) específica para esta materia.

La necesidad de esta directiva se justifica en el de hecho que no hay disposiciones horizontales sobre protección de infraestructuras críticas en la UE, motivo por el cual la Directiva establece un procedimiento de identificación y designación de infraestructuras críticas europeas, y un enfoque común para evaluar la necesidad de mejorar la protección de estas infraestructuras.

Entre las medidas sectoriales existentes en el sector de las tecnologías de la información figuran las siguientes:

1. La Directiva sobre el servicio universal (2002/22/CE) y la Directiva sobre la autorización (2002/20/CE), que tratan, entre otros aspectos, la integridad de las redes públicas de comunicaciones electrónicas.
2. La Directiva sobre la privacidad y las comunicaciones electrónicas (2002/58/CE), que trata, entre otros aspectos, la seguridad de las redes públicas de comunicaciones electrónicas.
3. Decisión marco 2005/222/JAI del Consejo, de 24 de febrero de 2005, relativa a los ataques contra los sistemas de información.
4. Reglamento (CE) 460/2004, de 10 de marzo de 2004, por el cual se crea ENISA.

La propuesta de directiva establece un procedimiento común para identificar y designar las infraestructuras críticas europeas, que son las infraestructuras cuya destrucción o interrupción afectaría a dos o más estados miembro, o bien a un único Estado miembro en el supuesto de que la infraestructura crítica esté en otro Estado miembro.

3.5_Divulgación y cooperación con la sociedad civil

Finalmente, un área de especial actuación es la que se centra en hacer llegar la seguridad de la información de forma efectiva a la sociedad civil. Muchos de los estados han iniciado actividades en este sentido.

Algunos de los ejemplos más relevantes en divulgación y cooperación son los siguientes:

- Asignación temporal de personal del sector privado en un centro de alta tecnología de lucha contra el cibercrimen (Australia).
- Creación de una asociación con entidades públicas, privadas y miembros de la sociedad civil para consolidar y desarrollar conocimiento sobre seguridad de las TIC (Austria).
- Actuación gubernamental como socio en actividades de divulgación (Austria, Australia, Canadá, Francia, Japón, Corea, España, Reino Unido o los Estados Unidos).
- Uso del esquema de certificación de la seguridad para llegar y concienciar al sector privado (Francia).

Las áreas de cooperación incluyen la seguridad de los sistemas y las redes de información, pero también la protección de las infraestructuras críticas, la lucha contra el cibercrimen o la certificación de la seguridad.

Con respecto a las actividades de divulgación, podemos encontrar en muchas modalidades: establecimiento de lugares y portales web (Japón, Noruega, España), seminarios dirigidos a usuarios generales de tecnologías de la información y a administradores de sistemas (Japón o Noruega) y campañas itinerantes (España, mediante la iniciativa de ASIMELEC, por ejemplo), campañas específicas sobre la cultura de la seguridad (Corea) y, finalmente, talleres de trabajo sobre aspectos concretos de seguridad (Francia).

3.5.1_*Actuaciones dirigidas a las pymes*

En relación con las pymes, una gran mayoría de estados han tomado ya iniciativas específicas para llegar: en algunos casos hay un diálogo con las asociaciones de pymes que ayuda a diseñar e implementar las iniciativas dirigidas a las pymes (Canadá, Dinamarca, Alemania), mientras que otra posibilidad es usar asociaciones publico-privadas específicas (Alemania o los Estados Unidos).

También encontramos iniciativas dirigidas a la vez a usuarios domésticos y a microempresas (Japón, Países Bajos, España, Suecia o los Estados Unidos).

En todos los casos, se considera esencial dirigirse a estos colectivos empleando un lenguaje que no sea técnico, aun cuando a la vez incluya terminología más técnica, que así irán conociendo.

Algunas de las iniciativas concretas son las siguientes:

- Poner información a disposición, tanto en línea como fuera de línea, como por ejemplo libros, manuales, guías, modelos de políticas y conceptos de seguridad, y perfiles de protección específicos para las pymes (Australia, Austria, Canadá, Alemania, Suecia, Reino Unido o los Estados Unidos).
- Establecer sitios web específicos para las pymes (Canadá, Alemania, Japón o Suecia).
- Ofrecer un sistema de alerta en amenazas emergentes dirigido específicamente a las necesidades de usuarios con poco o ningún conocimiento técnico (Alemania, Países Bajos, los Estados Unidos y recientemente España).
- Formación en línea para usuarios y administradores de sistemas (Corea, Estados Unidos y España).
- Seminarios, conferencias y talleres.
- Establecimiento de unidades específicas gubernamentales para ofrecer consejo técnico y asistencia a los fabricantes de tecnología de seguridad para incrementar la seguridad de sus productos y para facilitar el proceso de certificación (Francia).
- Hacer comprobaciones en línea sobre seguridad de las pymes (Corea).
- Ofrecer una herramienta en línea de autoevaluación para las pymes (Reino Unido).

- Desarrollar herramientas de software para facilitar la integración de la firma electrónica en los servicios y las aplicaciones de las pymes (Austria y más recientemente España).
- Obtener estadísticas sobre el estado de la seguridad de las pymes (Dinamarca).
- Ofrecer apoyo financiero y beneficios tributarios a la producción y adquisición de sistemas seguros (Japón).

3.5.2_*Actuaciones con el sector educativo*

Finalmente, hay que considerar varias actuaciones con el sector educativo en cuanto a seguridad de la información.

La mayoría de iniciativas tienen por finalidad educar a los niños y a los estudiantes a través de los maestros, profesores y familias o mediante la distribución directa de materiales informativos, incluyendo webs, juegos y herramientas en línea, postales, libros de texto y diplomas. Alguna iniciativa más puntual se dirige a formar personas grandes.

Algunas de las iniciativas concretas son las siguientes:

- Material de apoyo a maestros (Australia, Finlandia, Alemania, Países Bajos o los Estados Unidos) o inclusión de la seguridad en los programas educativos (España).
- Juegos en línea para público infantil, que suministran mensajes educativos sobre seguridad de la información (Australia).
- Control pedagógico y de seguridad a juegos con discapacitados (Alemania).
- Libros de texto y juegos dirigidos a niños (Corea).
- Diploma de uso seguro de Internet para jóvenes (Países Bajos o los Estados Unidos).
- Cursos a familias de estudiantes jóvenes para informar sobre la seguridad de la información (Países Bajos o los Estados Unidos).

En cuanto al alumnado de instituto y universidad, se pueden mencionar las iniciativas siguientes:

- Distribución de tarjetas postales con temática de seguridad (los Estados Unidos).

- Apoyo al alumnado de doctorado que prepara tesis de seguridad (Alemania), o en formación en el campo de la seguridad de la información (los Estados Unidos, con el programa Cyber Corps).
- Desarrollo de políticas de seguridad en las universidades (Canadá).
- Creación de una tarjeta electrónica de identidad, compatible con el esquema de la administración electrónica, con funciones de identificación y autenticación, firma electrónica, acceso físico, realización de fotocopias y copias, y cartera electrónica (Austria).

En relación con las personas grandes, hay algunas iniciativas para ofrecer información básica sobre seguridad de la información, como por ejemplo la iniciativa 21 de Alemana o la iniciativa de gente grande en red de Noruega.

Otras iniciativas de alcance general incluyen:

- Establecimiento de un centro de competencia para el aprendizaje de seguridad de nuevos medios (Alemania).
- Mantenimiento de una lista de cursos de formación ofrecidos por instituciones de enseñanza superior (Francia).
- Desarrollo de un CERT para instituciones educativas, con el mandato de gestionar incidentes de seguridad y diseminar informaciones sobre seguridad (Países Bajos, Finlandia).
- Celebración de jornadas como el Día de la Seguridad en Internet (Austria, Finlandia).
- Colaboración en redes de ámbito supraestatal, como la red europea de seguridad en Internet, la iniciativa dotSafe de la Red Europea de Escuelas o la red de seguridad, concienciación, hechos y herramientas (SAFT).

La Administración como impulsora del uso de herramientas de seguridad en las relaciones con la ciudadanía. La identidad y la capacidad electrónica

Ignacio Alamillo
Director de Asesoramiento e investigación de la Agencia Catalana de Certificación (CATCert)

1_LA SEGURIDAD DE LA INFORMACIÓN EN EL PROCEDIMIENTO ADMINISTRATIVO ELECTRÓNICO

Una de las fórmulas importantes para conseguir incrementar el nivel global de seguridad es la actuación de los estados y, en concreto, la incorporación de la seguridad al procedimiento administrativo electrónico, por el impacto directo e indirecto sobre la sociedad en su conjunto, indudablemente relacionado con el volumen del sector público sobre la economía.

En el capítulo anterior hemos presentado, de manera general, el conjunto de actuaciones y políticas públicas, mientras que en el presente exponemos algunas líneas gubernamentales internas de seguridad y, posteriormente, dos aspectos absolutamente estratégicos, como son la identidad y la capacidad electrónica, y las consideraciones correspondientes relativas a la privacidad.

1.1_Actuaciones gubernamentales para promover la seguridad del procedimiento administrativo

El estudio de la OCDE sobre la implementación de la cultura de la seguridad indica que un número importante de los estados disponen de políticas para la seguridad de la información dentro de las administraciones públicas (AP) (Australia, Austria, Canadá, Finlandia, Francia, Japón, Países Bajos, Suecia, Reino Unido, los Estados Unidos, República Checa, Portugal y República Eslovaca).

Mientras que al menos en cuatro estados esta política es específica y propia de la Administración, en otros casos se trata de una política que abarca tanto el sector público como el sector privado. En casi todos los casos la responsabilidad de coordinar la implementación de la política corresponde a una agencia o departamento ministerial concreto, con actividades que incluyen el desarrollo de políticas y normas, la coordinación

de su implementación o el ofrecimiento de consultoría, formación, auditoría e, incluso, selección de personal para las administraciones públicas.

Se pueden distinguir los siguientes tipos de iniciativas:

- Iniciativas de vigilancia y alerta y respuesta a incidentes de seguridad.
- Cumplimiento por parte de las AP de los estándares, recomendaciones o manuales de seguridad, especialmente los establecidos a partir de la norma ISO 17799.
- Desarrollo de una infraestructura de clave pública (PKI) para la comunicación con las AP y entre ellas.
- Desarrollo de software por parte des las AP, como por ejemplo aplicaciones de administración electrónica que hagan uso de la tarjeta de ciudadano, servicios de correo electrónico seguro o intercambio seguro de información por redes inseguras, con y sin cables.
- Servicios de pruebas de intrusión para las AP.
- Servicios de consultoría y formación para las AP.
- Desarrollo de redes seguras de comunicaciones para servicios, por ejemplo, de emergencia.
- Servicios centralizados de copia de seguridad para sistemas de información operados por AP.
- Implantación de proyectos de cooperación para dar a conocer la cultura de la seguridad entre las AP.
- Medición de la eficiencia de las políticas de seguridad y de su implementación, a partir de la realización de auditorías.

Asimismo, las anteriores actuaciones públicas internas están complementadas por iniciativas de cooperación y apoyo a las AP.

Estados como Austria, Australia, Canadá, Finlandia, Francia, Alemania, Japón, Corea, España, Suecia, el Reino Unido o los Estados Unidos, disponen de programas centrales dirigidos al resto de AP, regionales o locales.

Algunos de estos programas incluyen el establecimiento de órganos de coordinación con representantes de nivel regional o local (Australia, Austria, Canadá) y la preparación de guías de seguridad disponibles en las entidades locales (Austria, Finlandia, Japón).

Resulta notable la actuación legislativa de Francia, con una ley que obliga a las administraciones locales a considerar la seguridad de la información y a hacer análisis de riesgos antes de hacer comunicaciones por Internet.

La mayoría de los estados ofrecen formación específica en materia de seguridad y recursos de información a través de la Red para ofrecer apoyo a las entidades locales.

También resultan notables algunas iniciativas que ofrecen apoyo financiero a las entidades locales para la adquisición de equipamiento necesario para incrementar la seguridad de la información (Japón y Corea, entre otros).

Con respecto al Estado español, hay que mencionar la importante actividad que ha tenido el Ministerio de Administraciones Públicas en la creación de guías y normas de seguridad de la información en el procedimiento administrativo.

Resultan especialmente importantes las iniciativas siguientes:

- «Metodología de Análisis y gestión de riesgos en los sistemas de información» (MAGERIT), versión 2, elaborado por el Consejo Superior de Administración Electrónica. Sus objetivos son concienciar a los responsables de los sistemas de información de la existencia de riesgos y de la necesidad de corregirlos a tiempo, ofrecer un método sistemático para analizar estos riesgos y ayudar a descubrir y planificar las medidas oportunas para mantener los riesgos bajo control.
- «Criterios de seguridad, normalización y conservación en aplicaciones utilizadas para el ejercicio de potestades», de 2004, también elaborados por el Consejo Superior de Administración Electrónica. Sus objetivos son facilitar la adopción generalizada por parte de la Administración general del Estado de medidas organizativas y técnicas que aseguren la autenticidad, la confidencialidad, la integridad, la disponibilidad y la conservación de la información en las aplicaciones que esta emplea para el ejercicio de sus potestades; proporcionar el conjunto de medidas organizativas y técnicas de seguridad, normalización y conservación que garanticen el cumplimiento de los requisitos legales para la validez y la eficacia de los procedimientos administrativos de la Administración general del Estado que utilicen los medios electrónicos, informáticos y telemáticos en el ejercicio de sus potestades, y promover el máximo aprovechamiento de las tecnologías de la información y las comunicaciones en la actividad administrativa, a la vez que asegurar la protección de la información de los ciudadanos en sus relaciones con la Administración.

Aunque el alcance de las iniciativas mencionadas es la Administración general del Estado, en virtud del Real decreto 263/1996, es cierto que el

resto de administraciones las emplea como guía, voluntariamente, y amplía los aspectos que tratan, a menudo demasiado generales.

1.2_La seguridad y la confianza en la Ley de acceso electrónico en las administraciones públicas

Como es sabido, la existencia de políticas comunitarias y los compromisos oportunos de los estados miembro de cumplirlas, no obedece exactamente en ningún caso a la forma en la que se implementan dentro de cada Estado miembro, puesto que se considera que se trata de una decisión interna, que tiene mucho que ver con la configuración política de cada Estado, entre otros factores.

El recientemente discutido Anteproyecto de ley de acceso electrónico a las administraciones públicas recoge de manera importante las políticas comunitarias anteriores, y establece un calendario en línea con los compromisos asumidos por el Estado español en el marco del Plan de acción de administración electrónica i2010.

El modelo que establece el texto, en gran medida a instancia de las comunidades autónomas más adelantadas en la denominada administración electrónica y en línea de continuación de otras normas legales anteriores, como la Ley de firma electrónica, se basa en el hecho de que las comunidades autónomas son competentes para la organización y la prestación de los *servicios de seguridad y confianza* siguientes:

- Emisión de identidades digitales a ciudadanos y ciudadanas, así como a los órganos y autoridades de las administraciones públicas, a los trabajadores y trabajadoras públicos y a los dispositivos de producción de actos jurídicos administrativos automatizados, con garantía de reconocimiento mutuo.
- Determinación de los niveles de confianza de identidades digitales exigibles a los diferentes tipos de procedimientos administrativos y servicios públicos prestados por cada administración o entidad pública, puesto que es responsabilidad de cada organismo la determinación del medio más idóneo para cada caso concreto, incluyendo las condiciones adicionales al uso de la firma electrónica, como la acreditación de la competencia o de la capacidad jurídica de actuación (mediante apoderamientos y otros instrumentos).
- Admisión del uso y validación de identidades digitales emitidas por otros prestadores de servicios de certificación, públicos y privados,

en los procedimientos administrativos y servicios públicos, de acuerdo con las condiciones de seguridad y confianza anteriormente mencionadas, así como de acuerdo con criterios técnicos y económicos. Se podrán *federar* voluntariamente los sistemas de admisión de certificados y de firma electrónica.

- Emisión de sellos de fecha y hora, que acrediten el momento en el que existe un documento electrónico o en el que se ha producido un acto administrativo.
- Gestión de representaciones para autorización, que permite habilitar a personas o colectivos para tramitar en representación de terceros mediante autorizaciones concedidas electrónicamente mediante firma electrónica, sin necesidad de apoderamiento.
- Archivo electrónico seguro de documentos y expedientes administrativos, con la capacidad de preservarlos y mantenerlos accesibles durante plazos muy largos.

2_LA IDENTIDAD ELECTRÓNICA

Hoy, la mayoría de interacciones entre los ciudadanos, las empresas y las administraciones giran alrededor del concepto de identidad. Los gobiernos y el negocio afrontan la necesidad de identificar suficientemente a las personas, de manera fiable y correcta, para poder implantar sus procesos de negocio.

En esta sección presentamos la problemática y los retos de la gestión de la identidad electrónica, especialmente en el ámbito de las AP y, en concreto, de la Administración electrónica.

2.1_Concepto y tendencias en identidad electrónica

La identidad electrónica son los datos (a menudo denominadas atributos) que nos diferencian suficientemente del resto de personas o entidades, en un ámbito concreto, como por ejemplo, el nombre y apellidos, nombre del padre y de la madre, códigos de identificación, etc.

La identidad se asigna de acuerdo con las leyes, y puede estar acreditada mediante varios documentos:

- Identidad personal: partida de nacimiento, DNI, etc.
- Identidad corporativa: tarjeta de trabajador o funcionario, de profesional colegiado, de apoderado.
- Identidad de cliente, financiera, de fidelización, etc.

Todos tenemos muchas identidades, parciales, adecuadas a los diferentes roles y actividades que realizamos durante nuestra vida, y su uso está protegido por las leyes de protección de los datos de carácter personal, de manera particularmente intensa.

No se puede considerar que todas las identidades sean iguales, sino que las identidades que se nos asignan tienen cualidades diferentes y limitaciones de uso:

- Identidad de una web desconocida: no aporta ninguna garantía, y no se puede emplear a ningún efecto legal (pero puede resultar conveniente).
- Identidad de la banca electrónica: es razonablemente segura, pero sólo se puede emplear con quien la emite. Tiene potentes limitaciones de uso, atadas a las finalidades bancarias.
- IdCAT o DNI electrónico: son identidades muy robustas y fiables, emitidas con las garantías máximas legales. Se pueden emplear para todos los usos, y permiten *firmar electrónicamente*.

La necesidad de gestionar la identidad ha sido una de las necesidades más importantes de todos los sistemas de información, que habitualmente representan a las personas mediante un dato numérico o código. Si bien inicialmente cada sistema gestionaba la identidad de manera independiente, cada vez es más habitual implantar un modelo de gestión común a todas las aplicaciones de una organización concreta.

La gestión de la identidad y del acceso, a menudo conocida por su acrónimo anglosajón IAM (por *Identity and Access Management*), es el área de negocio que se dedica a las tareas siguientes:

- Aprovisionamiento de usuarios y contraseñas, mediante automatismos, de acuerdo con políticas de contraseña bien definidas y aplicadas. Así como, más recientemente, aprovisionamiento de certificados de firma electrónica.
- Implantación de sistemas de identificación y autenticación única corporativa (*single sign on*).
- Gestión centralizada de las atribuciones de los usuarios, basada en directorios.
- Modelo de autorizaciones, que concentra en un solo punto las autorizaciones de acceso.

La necesidad de negocio que cubre la gestión de identidad y de acceso es facilitar y controlar de manera eficiente los sistemas de identificación y

autenticación, el acceso y la auditoria (AAA) que emplean las organizaciones en sus procesos basados en tecnologías de la información.

La realidad tecnológica de las infraestructuras que apoyan a los procesos de tecnologías de la información, instaladas tanto en el sector público como en el sector privado, indica, sin embargo, que una parte muy importante de los sistemas sólo pueden emplear sistemas basados en contraseñas. No obstante, no parece que este obstáculo sea insuperable, y de hecho la industria de las tecnologías de la información ha proporcionado una serie de soluciones tecnológicas al problema, las más completas de las cuales están incluidas en la categoría de gestión de la identidad y del acceso.

Muchas entidades, públicas y privadas están preocupadas por la proliferación de cuentas de usuario y contraseñas, fenómeno que deriva de la necesidad impuesta a veces de manera artificial por muchas aplicaciones y sistemas de disponer de una cuenta de usuario y una contraseña para cada aplicación y sistema con el que se trabaja. Esta situación resulta difícil de controlar, puesto que cada proveedor de la Administración dispone de su propia tecnología, y decide si emplea o no autenticación certificada, y en definitiva el factor de decisión para la compra del producto es su funcionalidad y calidad, y no el sistema de autenticación empleado.

A esta situación hay que añadir la presión legal que supone la aplicación estricta de las leyes de protección de los datos de carácter personal, que obligan a un control de acceso detallado, e incrementa la aparición de más cuentas de usuario y contraseñas.

La solución más evidente a este problema es incorporar sistemas de autenticación basados en certificados y adicionalmente, cuando no se pueden eliminar las contraseñas, implementar procesos de *single sign on* basados en la tarjeta criptográfica:

1. Se crea un nuevo proceso en la organización, denominado *gestión de identidad y de acceso*.
2. Se adquiere un sistema de tecnología de la información que autenticará, en exclusiva, al usuario cuando acceda inicialmente al sistema. Se trata de una especie de *agente de usuario*, que lo representará ante el resto de sistemas.
3. Este agente conoce todas las contraseñas correspondientes a su usuario, puesto que se encuentran almacenadas de manera segura en un directorio.

4. Cuando hace falta acceder a una aplicación corporativa, es este agente quien se identifica ante la aplicación, sin volver a pedir la intervención del usuario.

El sistema de gestión se encarga, además, de todas las tareas asociadas a la gestión de todas las contraseñas de los usuarios. Por ejemplo, las políticas de seguridad de las aplicaciones normalmente determinarán la necesidad de renovar las contraseñas cada cierto tiempo. Estos sistemas lo hacen de manera automática, sin necesidad de intervención del usuario, que sólo se relaciona con su agente.

La evolución de este tipo de producto les ha llevado a ofrecer cada vez más funciones relacionadas con la seguridad, pasando de ofrecer soluciones estrictamente de gestión de la identificación y autenticación posterior (única) de los usuarios, a ofrecer soluciones centralizadas de las autorizaciones y de los permisos de los usuarios, y registro centralizado de los accesos (*audit*, en inglés).

Uno de los problemas y limitaciones de estos sistemas clásicos de gestión de la identidad reside en cómo gestionar la identidad a través de múltiples organizaciones.

Una solución bastante evidente, y que se ha aplicado en algunos dominios, especialmente dentro de las AP, es sencillamente crear y asignar una identidad a las personas que se pueda emplear (o incluso que haga falta hacerlo obligatoriamente) en todos estos dominios. La noción de un número DNI, NIF o de la tarjeta sanitaria responden a esta aproximación, puesto que son identificadores exclusivos de las personas.

Pero, tanto en el sector privado como en determinadas administraciones públicas, esta solución presenta limitaciones en cuanto a la conveniencia o capacidad legal de crear y asignar ulteriores códigos de identificación universal a los ciudadanos, y por otro lado, existen bastantes estados en los que la sensibilidad por la protección de los datos personales impide el establecimiento de esta clase de modelos. Austria, por ejemplo, pese a asignar un código único de identidad a todos los nacionales, prohíbe legalmente que este código sea empleado directamente, y se tiene que generar un código sectorial específico para su uso dentro de aquel sector, código que estará completamente disociado de otros códigos sectoriales, con la finalidad de impedir que se puedan cruzar datos del ciudadano a través de diferentes sectores.

Una segunda solución que ha aparecido más recientemente ante la problemática expuesta gira alrededor de la denominada *federación de identidades*, un entorno tecnológico, organizativo y jurídico que permite compartir la identidad y la autenticación de los usuarios entre varios sistemas, basado en normas de confianza mutua.

Algunos ejemplos son Liberty Alliance, GUIDE project, EEUU eAuthentication, Fidelity, que responden al fenómeno evidente de incremento de la complejidad de la identidad y de los mecanismos de autenticación que están asociados:

- Contraseñas, contraseñas dinámicas, contraseñas de un solo uso, basadas en hardware portátil (como tokens USB).
- Certificados digitales X.509 de identidad, emitidos por varios prestadores (por ejemplo, CATCert), a trabajadores públicos (CPISR) y a ciudadanos (idCAT), en especial en entornos de movilidad y de tramitación a distancia.
- Identificaciones electrónicas nacionales (DNI electrónico y otras).
- Tiques de autenticación remota/delegada (SAML).

Las soluciones de gestión y federación de identidad, muchas veces basadas en el estándar SAML, permiten que varios proveedores de identidad y de servicios puedan colaborar para llevar a cabo operaciones referidas a una persona, con control por parte de esta persona, del uso que se hace de su identidad y de los mecanismos de autenticación empleados. Como veremos posteriormente, también permite el control del intercambio de los atributos o datos personales adicionales.

Los casos de uso más habitual de SAML son los siguientes:

- **Single Sign-On:** durante los últimos años, varios productos han ofrecido soluciones privadas de autenticación única por la web (*Web Single Sign-On*), haciendo uso de *cookies* para el mantenimiento de la información de estado de la autenticación del usuario, de forma que no sea necesario volver a realizar la autenticación cada vez que el usuario accede a la web. Aún así, como las *cookies* no se comparten nunca entre dominios, estas soluciones han tenido que hacer uso de mecanismos privados y no estándares para ofrecer la autenticación única a múltiples dominios de seguridad. Aunque una solución basada en la tecnología de un proveedor único podría resultar aceptable dentro de una organización concreta, no resulta aceptable en el caso de transacciones con organizaciones diferentes, que pueden optar

por tecnologías diversas, ni en el caso de la relación con las AP. En este caso, el SAML se puede emplear como método normalizado para basar las soluciones de autenticación única a múltiples dominios.

- **Identidad federada:** cuando los servicios en línea necesitan establecer un entorno en el que los usuarios correspondientes de sus aplicaciones colaboren, estos sistemas deben tener una comprensión común sobre quién es el usuario que participa en la transacción. A menudo, los usuarios disponen de identidades locales diferentes dentro de cada organización y dominio de seguridad, de forma que se necesita una forma para compartir esta identidad y compartirla entre los diferentes dominios. Se dice que el usuario tiene una identidad federada cuando las organizaciones han llegado a un acuerdo sobre cómo identificar a un usuario. Desde una perspectiva administrativa, esta posibilidad de compartir la identidad del usuario permite reducir los costes de gestión de la identidad, puesto que los diferentes servicios a los que se conecta (por ejemplo las webs de las AP) no deben volver a obtener y gestionar los datos relativos a la identidad del usuario (como por ejemplo atributos identificadores o contraseñas). Además, los administradores de los servicios no necesitan establecer y mantener los mecanismos de identidad compartida, sino que lo puede hacer directamente el usuario afectado.
- **Aseguramiento de servicios web:** SAML permite el uso modular, que permite emplear, por ejemplo, el formato de aserción de manera desacoplada del protocolo. En concreto, cada vez resulta más frecuente el uso de SAML en servicios de autorización (iETF, Liberty Alliance y otras), marcos de trabajo sobre identidad y de servicios Web (OASIS XACML y WS-*, Liberty Alliance). En concreto, la especificación WS-Security de OASIS, que permite el aseguramiento de la mensajería SOAP, ha creado un perfil de servicio basado en la aserción SAML, que permite una forma más eficiente para el intercambio de atributos que otros perfiles del WS-Security.

Esta orientación de la federación de identidad ha generado la percepción de que la gestión federada puede ayudar de manera importante a la prestación de servicios públicos, especialmente en el entorno comunitario.

- Iniciativas de alcance europeo como FIDIS y MODINIS consideran la gestión de la identidad y las atribuciones como la solución a la integración de trámites a nivel europeo, de manera interoperable, especialmente teniendo en cuenta las identificaciones nacionales y regionales electrónicas (DNI, tarjetas sanitarias y otras).

- El proyecto GUIDE, construido siguiendo el modelo de intercambio de la iniciativa IDABC de la Comisión Europea, trabaja actualmente en perfiles y mensajería basados en SAML en un esquema de federación de las identidades europeas.
- Aparición de protocolos de negocio orientados a gestionar de manera altamente distribuida el control de acceso: permitirá que diferentes soluciones de gestión de la identidad colaboren, con base a servicios web (XACML).

Desde una perspectiva de la estrategia de las AP, el nuevo contexto de negocio se encuentra marcado por la heterogeneidad y la complejidad:

- Muchas identidades (pese a ser de más calidad): públicas, privadas, nacionales, regionales, locales, sanitarias, financieras... Tendencia a la reducción y generalización de las identidades (más DNI/idCAT, menos contraseña).
- Muchos proveedores en red sobre atribuciones y capacidades de personas: administraciones públicas, registros jurídicos y notariales, entidades privadas. Tendencia a la alta especialización y consumo en línea, mediante servicios web.

Este entorno nos lleva a la necesidad de establecer políticas públicas que, de manera progresiva, ofrezcan una respuesta suficiente a los retos que hemos visto, y que se pueden concretar en los siguientes puntos:

1. Validar varias identidades, generar evidencia y custodiarla.
2. Facilitar el acceso autenticado seguro e interoperable.
3. Gestionar personas, en lugar de identidades separadas.
4. Gestionar capacidades, personas que pueden hacer cosas.
5. Participar en esquemas de federación nacionales e internacionales. Por ejemplo, en Cataluña se podía promover un sistema catalán de federación de identidad, de manera alineada con el vigente Sistema de Certificación Pública de Cataluña, que regula la firma electrónica.

2.2_La política de la Unión Europea en gestión de la identidad

La Unión Europea ha ido perfilando la política sobre gestión de la identidad en una serie de instrumentos preparatorios, que interesa especialmente presentar.

[2003] La Administración electrónica y el futuro de Europa

La Comunicación de la Comisión en el Consejo, en el Parlamento Europeo, en el Comité Económico y Social y en el Comité de las Regiones, «El papel de la Administración electrónica en el futuro de Europa», COM (2003) 567, del 29 de septiembre de 2003, reconoce que sólo es posible ofrecer servicios públicos dentro de un entorno en la que exista confianza, entorno que debe garantizar siempre una interacción y un acceso seguro a empresas y ciudadanos.

La protección de los datos personales, la autenticación y la gestión de identidades son cuestiones básicas en las cuales ningún servicio público puede fallar, de forma que las instituciones públicas deben garantizar siempre la seguridad de las transacciones y de las comunicaciones digitales y la protección de los datos personales.

Los ciudadanos deberán tener siempre la posibilidad de controlar el acceso a sus datos personales, formas de almacenamiento y utilización de estos datos, así como de acceder a ellos.

La misma Comunicación indica que las estrategias de administración electrónica a todos los niveles deben promover la confianza en los servicios públicos, y que hace falta impulsar la gestión de la identidad dentro la Unión Europea, prestando especial atención a la interoperabilidad.

[2004] Retos para la sociedad de la información europea más allá del 2005

La Comunicación de la Comisión en el Consejo, en el Parlamento Europeo, en el Comité Económico y Social y en el Comité de las Regiones, «Retos para la sociedad de la información europea más allá del 2005», COM (2004) 757, de 19 de noviembre de 2004, identifica la necesidad de establecer políticas relativas al uso de las tecnologías de la información y las comunicaciones para cubrir carencias en los servicios públicos.

Entre otros, se identifican los siguientes problemas para tratar:

- Los problemas de gestión de la identidad.
- El grado insuficiente de seguridad y fiabilidad de las redes.
- La dificultad de poder enviar documentos firmados electrónicamente en el marco de los procedimientos telemáticos, especialmente en relación con las pymes.

[2005] i2010. Una sociedad de la información europea para el crecimiento y la ocupación

La Comunicación de la Comisión en el Consejo, en el Parlamento Europeo, en el Comité Económico y Social y en el Comité de las Regiones, «i2010. Una sociedad de la información europea para el crecimiento y la ocupación», COM (2005) 229, de 1 de junio de 2005, propone un marco estratégico, denominado i2010, que promueve una economía digital abierta y competitiva y que apuesta por las tecnologías de la información y las comunicaciones como impulsoras de la inclusión y de la calidad de vida.

Uno de los pilares en los cuales se basa este marco estratégico es la construcción de un Espacio Único Europeo de la Información, que se podrá construir si se superan cuatro grandes retos planteados por la convergencia digital:

- La velocidad de los servicios de banda ancha, para entregar servicios enriquecidos, como el vídeo de alta definición.
- La riqueza de los contenidos, incrementando la seguridad jurídica y económica para fomentar los nuevos servicios y los contenidos en línea.
- La interoperabilidad, potenciando los dispositivos y las plataformas capaces de hablarse entre sí, y los servicios transportables entre plataformas.
- La seguridad de Internet, para aumentar la confianza. Punto en que se considera una cuestión clave la gestión de las identidades.

[2005] Declaración ministerial de Manchester «Transformando los servicios públicos»

La Declaración de Manchester establece la necesidad de avanzar en el establecimiento, el reconocimiento y el funcionamiento interoperable de sistemas de identificación y autenticación de los ciudadanos y empresas, que maximicen la conveniencia y la facilidad de uso.

En este sentido, se identifica ya la necesidad de establecer políticas robustas de gestión interoperable de la identidad, así como la necesidad de crear un marco adecuado para la prestación de servicios de archivo seguro de documentos firmados electrónicamente.

[2006] Interoperabilidad de los servicios públicos paneuropeos de administración electrónica

La Comunicación de la Comisión en el Consejo, en el Parlamento Europeo, en el Comité Económico y Social y en el Comité de las Regiones,

«Interoperabilidad de los servicios públicos paneuropeos de administración electrónica», COM (2006) 45, de 13 de febrero de 2006, establece la necesidad de establecer un marco de colaboración en todos los niveles de administración para desplegar infraestructuras interoperables, desde las perspectivas siguientes:

- Interoperabilidad organizativa
- Interoperabilidad técnica
- Interoperabilidad semántica

La necesidad de interoperabilidad enmarca y limita la capacidad de las administraciones públicas de establecer sus estrategias de seguridad, identidad y firma electrónica, puesto que deben funcionar de manera conjunta con las iniciativas del resto de estados miembros, en especial en el futuro Espacio Único Europeo de Información previsto en la iniciativa i2010.

[2006] Plan de acción sobre Administración electrónica i2010: Acelerar la Administración electrónica en Europa en beneficio de todos

La Comunicación de la Comisión en el Consejo, en el Parlamento Europeo, en el Comité Económico y Social y en el Comité de las Regiones, «Plan de acción sobre Administración electrónica i2010: Acelerar la Administración electrónica en Europa en beneficio de todos», COM (2006) 173, de 25 de abril de 2006, establece medidas concretas en la ejecución del marco estratégico i2010, siguiendo la Declaración de Manchester, estructuradas alrededor de cinco grandes objetivos.

Entre estos objetivos, podemos encontrar el de establecer las herramientas clave que permitan disfrutar a ciudadanos y empresas, en el año 2010, de un acceso autenticado, cómodo, seguro e interoperable en los servicios públicos de toda Europa.

Las herramientas que se consideran clave son las siguientes:

- Gestión interoperable de la identidad electrónica para el acceso a los servicios públicos
- Autenticación de documentos electrónicos
- Archivo electrónico

La Comunicación indica también que el hecho de que existan iniciativas de tarjeta nacional de identidad, como es el caso del DNI electrónico español, es un tema diferente al de la gestión interoperable de la identidad electrónica para el acceso a los servicios públicos, considerando que

pueden existir conjuntamente, en especial porque la gestión interoperable de la identidad permite ofrecer servicios personalizados y más inteligentes, mientras que las tarjetas de identidad se dirigen a la lucha contra el terrorismo y el control de fronteras.

Resulta de especial interés que la Comunicación recuerde que cada Estado miembro debe decidir qué modelo de gestión interoperable de identidades desea implementar, y que será identificado posteriormente como un requisito del sistema europeo, «federado en sentido político».

2.3_El programa europeo de trabajo para la gestión interoperable de la identidad

Los estados miembro de la Unión Europea han firmado un documento, denominado «Acuerdo Signposts», que contiene un calendario ambicioso para alinear las actividades y los desarrollos en relación con los servicios de identidad, calendario que, pese a ser provisional, identifica una serie de elementos esenciales para la creación futura de un sistema de gestión europeo de identidad para toda Europa, y también establece hitos concretos que se consideran necesarios lograr, para garantizar que antes del 2010 se pueda conseguir el objetivo de los medios seguros de identificación electrónica que maximicen la conveniencia del usuario, a la vez que respeta las regulaciones de protección de datos personales.

Para concretar este acuerdo y este calendario provisional para la estrategia que hemos presentado anteriormente, la Comisión ha publicado una hoja de ruta de gestión interoperable de la identidad, cuyos principios se presentan a continuación:

1. **Usabilidad:** las consideraciones de usabilidad deberán ser las más importantes en la creación del marco de trabajo europeo de gestión de identidad, que significa que el sistema debe ser seguro, implementar las salvaguardas necesarias para proteger la privacidad del usuario y permitir el uso de acuerdo con los intereses y las sensibilidades domésticas.
2. **Identificación fuera de línea:** cada Estado miembro debería ser capaz de identificar a los usuarios dentro de sus fronteras, si desea que disfruten del acceso a servicios de gestión de identidad que estén en el extranjero. Para conseguir este objetivo, hace falta emplear identificadores adecuados de manera consistente que permitan la identificación y la autenticación precisas de los usuarios, así como el intercambio de información entre las AP en la medida necesaria para estos objetivos. Los requisitos fundamentales para un sistema que

satisfaga las necesidades de las personas físicas que debería ser ampliable a personas jurídicas.

3. **Identificación en línea**: cada Estado miembro tendría que emitir los mecanismos necesarios a sus usuarios, para que éstos puedan identificarse y autenticarse electrónicamente, como condición para tener acceso a servicios de gestión de identidad cuando estén en el extranjero. El usuario debe tener la capacidad de actuar de manera autónoma y de hacer uso de los servicios ofrecidos.
4. **Apoderamientos y autorizaciones:** cada Estado miembro tendría que ofrecer los mecanismos para gestionar las competencias y capacidades de los usuarios identificados dentro de sus fronteras, siempre que estas autorizaciones no se encuentren legalmente sujetas a aprobación por las autoridades de otro Estado miembro.
5. **Validación en línea:** cada Estado miembro tendría que ofrecer servicios en línea de validación de las identidades, competencias y autorizaciones, si desea ofrecer servicios de gestión de identidad.
6. **Consenso:** hay que establecer un consenso de alto nivel entre los estados miembro sobre la terminología de gestión de identidad para garantizar la interoperabilidad conceptual y semántica, consenso que se podría confirmar mediante medidas políticas y legales apropiadas.

A partir de estos principios básicos, de la hoja de ruta derivan una serie de criterios de diseño para el sistema europeo de gestión de identidad, que también se encuentran en el acuerdo Signposts, con una orientación muy clara de la interoperabilidad del sistema, que debería:

1. Ser federado en un sentido político, por ejemplo, permitiendo a las AP confiar mutuamente en los métodos de identificación y autenticación empleados, aceptándolos en la jurisdicción en la que se lleva a cabo el procedimiento siempre que también sean aceptables en el Estado de origen.
2. Ser multinivel, en el sentido de que los estados miembro deberían poder ofrecer múltiples niveles de seguridad para los servicios de gestión de identidad, de forma que los requisitos de autenticación para cada servicio de Administración electrónica puedan ser ajustados a las necesidades de seguridad de aquel servicio. Los estados miembro son los que deciden a qué nivel quieren ofrecer los servicios de autenticación, y cuál es el nivel de autenticación que se necesita para cada servicio, aunque han de aceptar como válido cualquier método de autenticación de este nivel suministrado por el resto de los

estados miembro. Esto implica definir un conjunto de criterios a escala europea para cada nivel de autenticación.

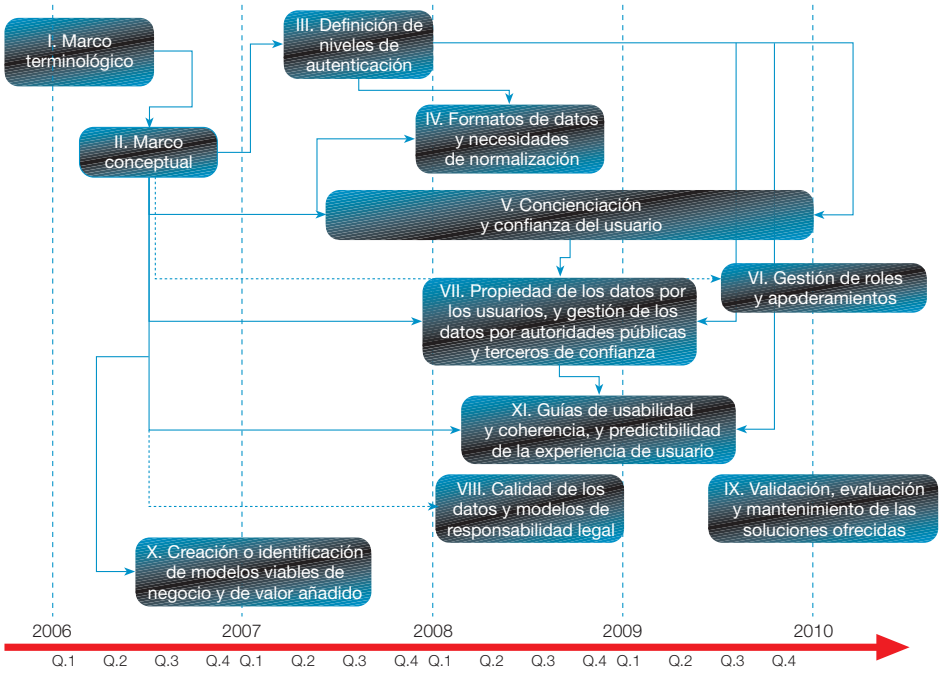
3. Confiar en fuentes de información auténtica. Para garantizar la calidad de los datos y la eficiencia de la Administración electrónica, tendría que existir al menos una fuente única y auténtica para cada punto de información de cada entidad registrada en el Estado miembro de origen, que puede ser una base de datos o un *token* (como un certificado).

4. Permitir una aproximación basada en sectores o contextos diferentes, cuando esto sea deseable para el Estado miembro de origen, y que de hecho supone una extensión lógica del modelo federado.

5. Permitir el desarrollo del mercado privado, en los casos en que los estados miembros decidan confiar en socios del sector privado (como por ejemplo entidades financieras) para la provisión de servicios de gestión de identidad a los usuarios.

La orientación federada del modelo tiene como objetivo la provisión de servicios de forma respetuosa con el mercado único y con los objetivos de Lisboa, pero respetando la autonomía de los estados en cuanto al segundo y tercer pilar, así como sus prioridades políticas domésticas.

Entrando algo más en detalle dentro de la hoja de ruta, encontramos 11 fases de trabajo, que se organizan como muestra el gráfico siguiente:



El objetivo de cada fase de trabajo se expone a continuación:

1. Marco terminológico: actualmente, los estados miembro han implementado o se encuentran en fase de implementación de infraestructuras nacionales de gestión de identidad, sin que exista un acuerdo común sobre la definición de conceptos esenciales, como identidad, entidad, atributo, delegación o, incluso, autenticación de entidad o gestión de identidad. Como resultado se podrían producir problemas importantes a nivel europeo, puesto que la ausencia de una comprensión común del problema puede impedir los acuerdos necesarios para que estas infraestructuras resulten interoperables. Esta terminología debería ser neutral filosófica y técnicamente, y abarcar las nociones más habituales.
2. Marco conceptual: para avanzar hacia cualquier actividad de implementación es importante tener una visión muy clara y un consenso substancial en relación con la organización y los principios básicos que deben gobernar la arquitectura europea de gestión de identidad. Esta fase precede a la respuesta a cuestiones más prácticas para la implementación, como cuáles son las elecciones técnicas que hay que realizar, o la identificación de los responsables de la creación y gestión de cada componente de la infraestructura. Este marco conceptual debe constituir un modelo de alto nivel de la infraestructura prototipo del sistema. Construido sobre el marco terminológico, el marco conceptual tendrá que indicar los principios básicos de la infraestructura y suministrar los requisitos que deben cumplir las tareas de implementación.
3. Definición de niveles de autenticación: esta fase incluye la definición de un conjunto de niveles de autenticación, empleando estándares concretos, que describe diferentes niveles de seguridad que pueden ser utilizados para comparar los niveles de seguridad que ya han establecido los estados miembro, y para establecer un nivel de seguridad apropiado para un servicio de Administración electrónica, que será común para toda la Unión Europea. Para eso hace falta analizar tanto los procedimientos de registro como los procedimientos de autenticación.
4. Formatos de datos y necesidades de normalización: a partir de la amplia variedad de soluciones de gestión de identidad implantadas a nivel nacional y de la poca probabilidad de implementación de un *token* europeo único (una tarjeta de ciudadano europeo, por ejemplo), la infraestructura europea de gestión de identidad deberá garantizar la lectura y el intercambio de datos de usuario, tanto de manera local (por ejemplo, mediante un *token*) como a distancia (por ejemplo, con-

fiando en fuentes auténticas de información a nivel nacional cuando estas informaciones no estén almacenadas en el *token*), siempre cumpliendo las normas de privacidad. Para cumplir estos requisitos, algunos estándares tendrán que ser aceptados por formatos de datos y por los procesos de intercambio de datos.

5. Concienciación y confianza del usuario: la confianza y la concienciación son dos condiciones previas que se considera básico satisfacer, pero que se encuentran muy atadas a la organización y al funcionamiento del proveedor del sistema de gestión de identidad, y que por lo tanto son una pieza clave de la hoja de ruta. Sin confianza en la seguridad del sistema y concienciación de los principios operativos básicos del sistema y de sus garantías, probablemente el sistema no será empleado por los usuarios, o será percibido como una intrusión negativa, en vez de como un beneficio.
6. Gestión de roles y apoderamientos: la representación de otra persona puede ser impuesta por la ley o establecida contractualmente. Algunos ejemplos incluyen la representación de los menores de edad o de los discapacitados o la representación empresarial, con intervención notarial. El modelo europeo de gestión de identidad debería garantizar la creación e implementación de una infraestructura federada viable que permita a un prestador de servicio verificar que una tercera persona ha recibido la representación de un usuario, cuando esto sea aceptable de acuerdo con la ley del Estado de origen.
7. Propiedad de los datos por los usuarios, y gestión de los datos por autoridades públicas y terceros de confianza: los usuarios finales deben tener el máximo grado de control sobre sus datos personales en el sistema europeo de gestión de identidad, siguiendo un modelo mixto de autorización, voluntaria e involuntaria, de los datos personales, en el que el usuario autoriza a un intermediario el acceso a sus datos personales por parte de un prestador de servicios, bien de manera voluntaria u obligatoria en casos excepcionales (como por ejemplo emergencias sanitarias o de seguridad nacional). Lo que resulta más importante es que el usuario tenga un suficiente grado de control y conocimiento de sus datos a los que accede el prestador del servicio, teniendo en cuenta el principio de proporcionalidad de la legislación de privacidad. El control de los datos personales implica una participación activa por parte del usuario, en la emisión, la extensión, la restricción y la retirada de credenciales, y en la gestión de los datos personales, incluyendo el acceso y la actualización de datos

personales tanto como sea posible, para garantizar siempre que los datos en las fuentes auténticas sean tan precisos como se pueda.

8. Calidad de los datos y modelos de responsabilidad legal: la disponibilidad de fuentes auténticas de datos implica que cada atributo debería ser almacenado sólo una vez, al menos idealmente, y que los usuarios no deberían suministrar un dato más de una vez. Para que este sistema funcione a escala europea, los estados miembro deben ser responsables de la calidad de los datos, en relación con los datos gestionados por sus sistemas y, todavía más, los estados deben ser responsables de manera objetiva de la corrección y precisión de los datos, puesto que estas garantías legales son la base de la confianza en los modelos de identidad federada. Hay que recordar que todo tratamiento de los datos se deberá hacer de acuerdo con la normativa de protección de los datos de carácter personal.
9. Validación, evaluación y mantenimiento de las soluciones ofrecidas: para cumplir el Plan de acción de administración electrónica no sería suficiente establecer de la infraestructura de gestión de identidad sin un seguimiento posterior. Hace falta evaluar de manera periódica la idoneidad de la infraestructura, para garantizar que las soluciones ofrecidas a escala nacional cumplen las guías europeas, y que satisfacen las expectativas de los usuarios a la vez que los requisitos de seguridad. Sólo de esta forma se puede garantizar la confianza suficiente por parte del usuario.
10. Creación o identificación de modelos viables de negocio y de valor añadido: una vez establecido el marco de trabajo, la prioridad principal debería ser la identificación e implementación de aplicaciones clave, combinando resultados rápidos y proyectos a gran escala.
11. Guías de usabilidad y coherencia, y predictibilidad de la experiencia de usuario: la confusión de los usuarios finales puede comportar una confrontación de sistemas con diferentes interfaces informáticas, que impida identificar al usuario que está realizando una misma tarea.

La hoja de ruta que hemos presentado se encuentra actualmente en las etapas iniciales, con una actividad intensa tanto en la Unión Europea como en las administraciones estatales. En el Estado español no se ha producido a fecha de hoy un debate sobre el modelo de gestión y federación de identidad, sino que todos los esfuerzos de la Administración central parecen centrados en la promoción del DNI electrónico que, pese a ser una parte de la solución, no es la más importante en nuestra opinión.

Hace falta, por lo tanto, profundizar en la definición de este modelo y explorar el papel que deben tener en este sistema las comunidades autónomas, las empresas y los ciudadanos.

3_LA ACREDITACIÓN ELECTRÓNICA DE LA CAPACIDAD

Como se ha presentado anteriormente, uno de los aspectos esenciales para permitir la actuación de las personas es la acreditación electrónica de su capacidad jurídica y de obrar, mediante diferentes técnicas, como por ejemplo la incorporación de informaciones específicas en los certificados digitales de identidad, en bases de datos o, más recientemente, en sistemas de gestión de identidad que funcionan de manera conectada.

Ya habíamos indicado anteriormente que aunque la gestión de la identidad representa una oportunidad importante para las AP y para los prestadores de servicios de certificación, no es menos cierto que la regulación de los trámites y de los procedimientos administrativos realizados mediante las tecnologías de la información y la comunicación no debe limitarse a una simple reproducción o adaptación del elemento presencial en la utilización de estos nuevos medios, sino que se han de aprovechar al máximo las posibilidades que los mencionados medios ofrecen para que, con todo el respeto al principio de seguridad jurídica, se pueda establecer un marco jurídico que no sólo asegure y fomente la utilización de las TIC, sino que también resulte eficiente y ventajoso para la Administración, el ciudadano y la empresa.

Precisamente los últimos adelantos de las TIC, y en especial los producidos con la *Web semántica*, que se relacionan directamente con el uso de las firmas electrónicas, ofrecen oportunidades reales para eliminar la necesidad de solicitar a los ciudadanos y empresas los documentos acreditativos de sus facultades y capacidades (en especial, derivadas de apoderamientos voluntarios y de situaciones orgánicas, como los cargos en las empresas y otras entidades), y posteriormente comprobarlos.

En definitiva, se trata de pasar de un modelo en el que simplemente se gestionan las diferentes identidades de los ciudadanos y empresas, a un modelo en el que se gestionan, además, sus diferentes capacidades de actuación jurídica.

Conseguir implantar estas tecnologías y métodos en los procedimientos administrativos comportará una simplificación importante en la tramitación formal, así como una reducción considerable de los documentos que

forman el expediente, sin ninguna reducción de las garantías jurídicas, hecho que justifica este cambio de paradigma, con el paso de la gestión de la identidad a la gestión de las capacidades jurídicas personales.

Este modelo requiere elementos técnicos, que se construyen sobre las tecnologías de base de la firma electrónica y de la gestión de la identidad, así como elementos de organización, dirigidos a la disposición concreta y la organización de los medios materiales de que dispone la Administración, con el objeto de abarcar la eliminación total de los documentos (en papel o electrónicos) que ofrecen pruebas, dentro de los expedientes, de la identidad del ciudadano o empresa, y de su capacidad para actuar en el procedimiento.

Las modalidades de capacidad electrónica que hay que considerar incluyen, al menos, las siguientes:

- Actuación en nombre propio (personas físicas, personas jurídicas y entidades sin personalidad jurídica).
- Actuación como representante voluntario, de persona física o de persona jurídica o entidad sin personalidad jurídica, en función de las facultades concedidas.
  - Actuación como apoderado notarialmente.
  - Actuación como autorizado, con y sin comprobación previa de la autorización.
- Actuación como representante orgánico, en función de los roles legales establecidos en cada persona jurídica o entidades sin personalidad.

La implantación del modelo de gestión de identidades y capacidades requiere el desarrollo de plataformas específicas, de las cuales el proyecto PASSI de CATCert es un ejemplo.

El Plan estratégico de proyectos de la Administración Abierta de Cataluña para el período 2005 identificó la necesidad de que CATCert desarrollara una infraestructura de gestión de las diferentes identidades y atribuciones que los ciudadanos y las ciudadanas de Cataluña han de emplear para relacionarse con las diferentes administraciones, con el objetivo de unificar y simplificar la gestión.

La Plataforma de Atributos de Seguridad y Firma Electrónica (PASSI) debe cubrir las necesidades anteriormente identificadas, con base en los servicios de identidad y validación semántica de CATCert, ofrecidos por la Plataforma de Servicios de Identidad y Firma Electrónica (PSIS), que además obtiene y archiva las correspondientes evidencias electrónicas.

Las funciones principales que forman parte del sistema PASSI son:

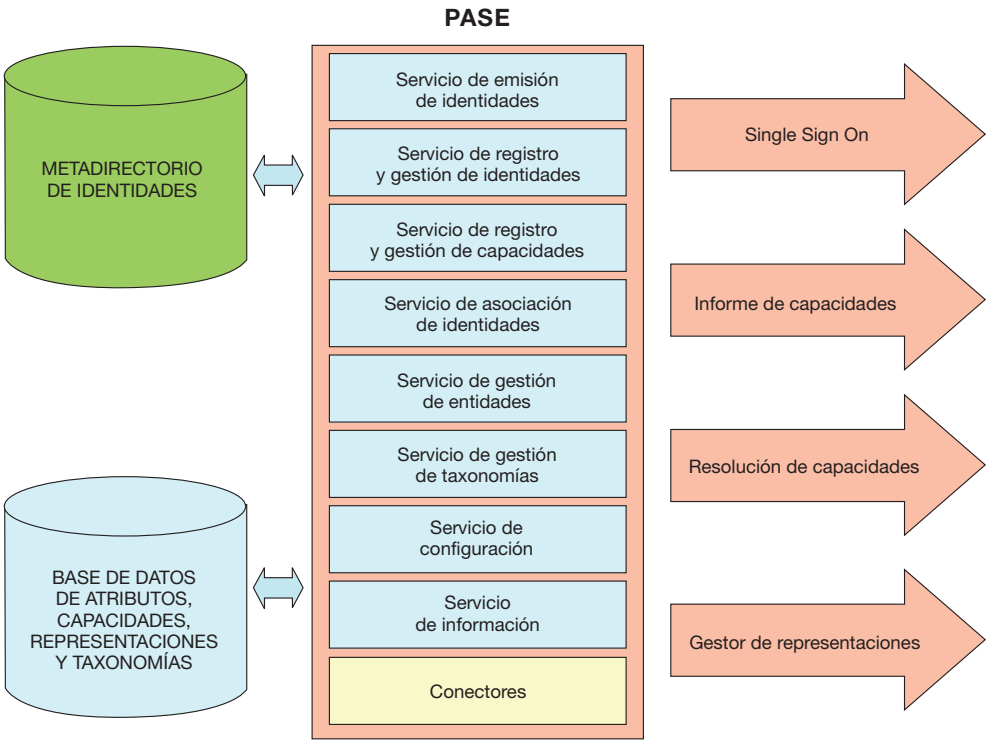
1. Almacenamiento de las identidades que han sido aprovisionadas por CATCert, mediante sus diferentes servicios (incluyendo los certificados), que serán empleadas en procedimientos de autenticación única (*single sign on*) o autenticación federada (Liberty o SAML), o en procedimientos de firma electrónica.
2. Almacenamiento y relación de las identidades aprovisionadas por terceras entidades, públicas y privadas, de forma que el usuario pueda decidir qué identidades emplea para cada caso y entidad (identidad federada).
3. Permitir la carga de información de representantes, actuando como depósito de información del gestor de representaciones.
4. Permitir la gestión de perfiles, roles y relaciones de representación de los usuarios, y la asignación de autorizaciones de acceso a los sistemas, de acuerdo con el modelo de datos de PASSI y con las políticas de seguridad correspondientes, así como el registro de aserciones de acceso con garantía de sellado de fecha y hora.
5. Permitir la integración con directorios de usuarios, mediante procedimientos de réplica, sincronización y federación, dentro de un concepto amplio de metadirectorio de ciudadanos y empresas.
6. Permitir que las AP deleguen a CATCert partes del proceso de decisión del control de acceso a los sistemas, aplicaciones y recursos, incluyendo registros públicos, mediante la ocupación del estándar XACML. En este caso, la Administración hace a CATCert una pregunta del tipo «¿puede esta identidad hacer este acto en nombre de?».

La plataforma PASSI ofrece cuatro grandes aplicaciones, la funcionalidad de las cuales quedará definida en este pliego:

- Aplicación de Web Single Sign On, que se ofrecerá a las diferentes administraciones, organizaciones o departamentos interesados, para asegurar que las personas que acceden a los diferentes sistemas presentan o conocen las credenciales adecuadas para acceder a los diferentes sistemas.
- Aplicación del informe de capacidades, que tendrá que informar a las diferentes entidades usuarias si el usuario que quiere hacer un determinado trámite tiene las capacidades necesarias para hacerlo.

- Aplicación de resolución de capacidades, que deberá comprobar, a través de información almacenada PASSI o a través de consultas con otras entidades, las capacidades o atribuciones que los usuarios declaren poseer. Para esto último hace falta la creación de conectores para acceder a las diferentes fuentes de información que puedan proporcionar conformidad sobre las capacidades alegadas.
- Aplicación de gestión de representaciones que asume las funciones de permitir a los usuarios finales identificados el otorgamiento en línea o la adquisición a terceros de informaciones de capacidades de otros usuarios. A las administraciones, les permitirá la carga de estas mismas informaciones, a partir de procesos de validación.

A continuación mostramos el conjunto de servicios de la plataforma PASSI, en apoyo a estas aplicaciones:



Para ofrecer estos servicios, PASSI hace uso de un modelo de web semántica aplicado a la gestión de la identidad y las capacidades, basado en estándares internacionales, con los objetos siguientes:

- Persona
- Relación
- Entidad
- Facultad
- Acto
- Procedimiento

El objeto «Persona» describe cualquier identidad de una persona física. Puede tratarse de una identidad basada en un nombre de usuario/contraseña o en un certificado. Cuando la identidad se basa en nombre de usuario/contraseña, la representación se limita a una credencial SAML (los datos de identificación de la persona dentro del elemento «subject» de la manifestación, asociado al emisor de esta identidad, que debe figurar en el documento SAML como «issuer» de la manifestación). Cuando la identidad se basa en un certificado, puede haber sido generada por cualquier prestador de servicios de certificación.

El objeto «Entidad» describe cualquier identidad de una entidad diferente a la de una persona física. Habitualmente se trata de instituciones, personas jurídicas públicas y privadas, y entidades sin personalidad jurídica propia. Las «entidades» no actúan en el tráfico, sino que lo hacen a través de personas físicas, como es tradicional en nuestro sistema jurídico.

El objeto «Relación» describe una relación concreta entre dos personas o una persona y una entidad. Comprende los objetos correspondientes, e información adicional sobre la relación. Cuando resulta pertinente, como en los casos de representación voluntaria, la relación indica la lista de facultades concretas para las cuales resulta válida la relación. En principio se han considerado los tipos de relaciones siguientes, aunque el esquema debe permitir establecer tipos adicionales:

1. Relación basada en la simple vinculación entre la persona y la persona/entidad.
2. Relación basada en la representación legal entre la persona y la persona/entidad.
3. Relación basada en la representación orgánica entre la persona y la persona/entidad.
4. Relación basada en la representación voluntaria entre la persona y la persona/entidad.

5. Relación basada en la representación presunta entre la persona y la persona/entidad.

El objeto «Facultad» describe una facultad concreta de una persona, establecida por una autoridad concreta. Esta autoridad puede ser, por ejemplo, una AP, un notario u otra similar. Las facultades pueden presentar límites, y hay que definir los tipos de límites.

El objeto «Acto» describe una acción concreta, un trámite que hay que efectuar. Se relaciona con los anteriores de la manera siguiente:

1. Acto realizado por una persona P, en su propio nombre y representación.
2. Acto realizado por una persona P para otra persona P en virtud de una relación R(PRP).
3. Acto realizado por una persona P para una entidad (E) y en virtud de una relación R (PRE).

El objeto «Procedimiento», finalmente, describe series ordenadas de actos, en forma de flujos de trabajo.

Hay que remarcar que PASSI no es un depósito único de identidades y facultades, no sólo por su complejidad técnica, sino especialmente por la compleja cobertura legal que requeriría.

Al contrario, PASSI se basa en el establecimiento de unas bases jurídicas, organizativas y técnicas que permiten la interconexión de varios registros pertenecientes a diferentes sujetos públicos, y define los procedimientos de consulta en línea de las facultades, con respeto total a la finalidad del registro público y a la protección de los datos de carácter personal. Por otro lado, este modelo permite la evolución de los modelos de negocio de los diferentes proveedores de la información, y supera la todavía existente dicotomía copia simple/certificado, con efectos jurídicos diferentes (así como, en algunos casos, tasas o aranceles diferentes), que, además, únicamente ofrecen garantía en relación con el momento inmediatamente posterior a la emisión de la copia o certificado (sin perjuicio de la presunción de vigencia que pueden llevar adjunta).

4_LA PRIVACIDAD EN LOS SISTEMAS DE IDENTIDAD DE CAPACIDAD ELECTRÓNICA

La privacidad actúa como límite de especial relevancia en relación con los sistemas de identidad y de capacidad electrónica, por las consecuencias potenciales de la identificación masiva de las personas y la

disposición de redes públicas que permiten el acceso a todas las bases de datos públicas con informaciones de estas personas.

Por este motivo, es especialmente importante que los sistemas de identidad y capacidad electrónica permitan la participación de las personas identificadas y, lo que es más importante, el control por parte de estas personas del acceso a los datos y la autorización para el intercambio en línea de sus datos, siempre de acuerdo con los estándares legalmente determinados de acuerdo con la legislación aplicable, hecho que también comporta un reto adicional en las relaciones con el elemento internacional.

Las tecnologías emergentes de identidad y capacidad electrónica han considerado la privacidad como un elemento nuclear de sus propuestas, como podemos ver a continuación, introduciendo las propuestas de Microsoft y de Liberty Alliance, dos de las más importantes.

4.1_Las 7 leyes de la identidad

Una de las propuestas conceptuales interesantes para conciliar los sistemas de gestión de identidad y capacidades con la privacidad es la propuesta de las denominadas *7 leyes de la identidad*, que hay que entender en el sentido de principios, propuesta adoptada ya por algunas instituciones relevantes en el ámbito de la protección de datos personales (por ejemplo, Canadá), que establece las condiciones siguientes:

- **Ley 1:** Control y consentimiento del usuario. Los sistemas de identidad técnica sólo deberán divulgar información identificativa de un usuario con su consentimiento.
- **Ley 2:** Divulgación mínima para uso restringido. La mejor solución a largo plazo es la que divulga la menor cantidad de información de identidad posible y la que mejor limita el uso posterior.
- **Ley 3:** Justificación de los terceros. Los sistemas de identidad digital deben estar diseñados de forma que la divulgación de información identificadora se encuentre limitada a terceros que tengan una posición justificada y fiable en una relación de identidad concreta.
- **Ley 4:** Identidad dirigida. Un sistema de identidad universal ha de ofrecer apoyo tanto a identificadores *omnidireccionales* para el uso en entidades públicas, como identificadores *unidireccionales* para el uso en entidades privadas, y facilitar el descubrimiento a la vez que prevenir la divulgación innecesaria de las correlaciones de la identidad.

- **Ley 5:** Pluralismo de tecnologías y operadores. Un sistema universal de identidad debe canalizar y habilitar el funcionamiento conjunto de servicios de varios operadores basados en múltiples tecnologías de identidad.
- **Ley 6:** Integración humana. El sistema de identidad debe definir al usuario humano como un componente del sistema distribuido, integrado en este mediante mecanismos de comunicación hombre-máquina con protección frente a ataques de identidad.
- **Ley 7:** Experiencia consistente en todos los contextos. El sistema debe garantizar a los usuarios una experiencia simple y consistente, pese a permitir la separación de contextos de múltiples operadores y tecnologías.

El modelo de gestión de identidad de la tarjeta de información (*Information Card*), en el que se basa la propuesta Microsoft CardSpace, se basa en las 7 leyes de la identidad y ofrece un ejemplo de cómo cumplirlas.

En este sistema, de acuerdo con la Ley de control y consentimiento del usuario, este será el responsable de seleccionar y enviar un conjunto suficiente de alegaciones de identidad a los destinatarios que las deberían usar, siempre que consideren que pueden confiar en ellos. Si el usuario no se siente cómodo divulgando la información personal asociada a una tarjeta de información concreta, puede decidir no utilizarla.

Los usuarios también pueden crear tarjetas de información propias, sin necesidad de proveedores externos de identidad, aunque en este caso evidentemente la información tendrá un valor diferente para el destinatario, que no siempre confiará en las alegaciones hechas por el usuario.

Por otro lado, de acuerdo con la Ley de pluralismos de tecnologías y operadores, los usuarios podrán construir múltiples identidades digitales, diferentes en cuanto a la cantidad y a la calidad de la información, de modo que cada usuario tenga una serie de tarjetas de información en su cartera virtual, que permitirá que el usuario seleccione la tarjeta más apropiada para cada destinatario, controlando de manera efectiva su información.

Mientras que algunas tarjetas no contendrán ningún dato nominativo, sino atributos como el sexo o la edad, otras podrán contener más o menos datos nominativos, para hacer transacciones con las AP por vía electrónica, por ejemplo, cumpliendo las leyes de divulgación mínima y justificación de terceros. La capacidad de crear y emplear múltiples tarje-

tas por parte del usuario lo protege de la creación de perfiles, hecho que cumple la Ley de la identidad dirigida.

4.2_La privacidad en las federaciones de identidad

Hemos presentado anteriormente el estándar SAML, promovido por OASIS, que se encuentra en el núcleo de los sistemas de gestión y federación de identidad. Se ofrecen un número de mecanismos que ofrecen apoyo a la privacidad de los usuarios:

- SAML permite el establecimiento de pseudónimos entre un proveedor de identidad y un proveedor de servicios. Estos pseudónimos no permiten, por sí mismos, establecer una correlación inapropiada entre dos proveedores de servicios diferentes, como sí que sería posible en caso de que el proveedor de identidad usase un identificador único o global, como por ejemplo el DNI electrónico.
- SAML permite identificadores transitorios o de un uso, que garantizan que cada vez que un usuario concreto accede a un proveedor de servicio a través de una operación de autenticación única con la intermediación de un proveedor de identidad, lo hace con una nueva *identidad*, de forma que el proveedor de servicio no podrá reconocerlo.
- Los mecanismos de contexto de autenticación de SAML permiten a un usuario ser autenticado a un nivel de seguridad suficiente, pero no excesivo, apropiado a la política aplicable al recurso al que se accede.
- Finalmente, SAML permite expresar entre proveedores el hecho de que un usuario han consentido determinadas operaciones, por ejemplo el acto de federación de identidades entre dos proveedores.

Por otro lado, Liberty Alliance, la asociación global que promueve normas y estándares de federación de identidad, que emplea y amplía el estándar OASIS, ha diseñado los sistemas pensando en la protección de los datos personales, considerada como pieza fundamental en la confianza de los usuarios.

La elección y el consentimiento por parte del ciudadano son los aspectos esenciales en la visión de Liberty Alliance. El marco general de las especificaciones técnicas de Liberty se ha construido partiendo de la base que la información personal será compartida en el contexto del consentimiento del usuario, y de acuerdo con sus instrucciones. Esto implica, además de la posible regulación previa entre los proveedores que intercambian la información del usuario, informarlo y obtener su consentimiento expreso.

Las especificaciones de Liberty permiten el almacenamiento de este acto de información al usuario y de su consentimiento.

Para reforzar esta noción y respetar la privacidad de los usuarios, Liberty Alliance ha publicado una serie de recomendaciones más detalladas:

- **Información.** El sistema del usuario que se relaciona con los proveedores de identidad o de servicio que hacen uso de las especificaciones de Liberty han de informar a la persona afectada sobre quién obtiene la información, qué información obtiene, cómo se obtiene la información (por ejemplo, directamente o a través de *cookies*), cómo los proveedores tratan los principios de elección, acceso, seguridad, calidad, relevancia, etc. de los usuarios, si divulgan la información a otras entidades o si actúan por cuenta de terceros.
- **Elección.** El sistema ha de ofrecer a los usuarios elecciones, hasta donde resulte adecuado de acuerdo con las circunstancias, en relación con qué información personal se capta y cómo será tratada más allá de la finalidad para la cual se capta. Adicionalmente, el sistema debería permitir a los usuarios revisar, verificar o actualizar los consentimientos que ya hayan dado o denegado previamente.
- **Acceso de los usuarios a su información personal.** El sistema debería permitir, de acuerdo con la legislación aplicable, como es el caso español, un acceso razonable a su información personal captada directamente u obtenida a través de terceros.
- **Calidad.** El sistema debería permitir a los usuarios una oportunidad razonable, que de acuerdo con la ley aplicable puede ser obligatoria, de corregir la información personal almacenada por los proveedores.
- **Relevancia.** Los proveedores deben usar la información personal para las finalidades para las cuales se obtuvo la información, de acuerdo con la ley aplicable.
- **Plazo.** Los proveedores no deben retener la información personal durante un plazo superior al necesario y aceptado o solicitado por el usuario.
- **Resolución de disputas.** Los proveedores han de ofrecer mecanismos de resolución de disputas, cuando sea posible y sin perjuicio de la ley aplicable.
- **Seguridad.** Los proveedores deben proteger los datos con un nivel de seguridad adecuado, a menudo determinado reglamentariamente.

Finalmente, las especificaciones de Liberty Alliance ofrecen algunas herramientas interesantes para poder cumplir estos compromisos, que permiten incrementar la capacidad de elección y el control de un usuario en relación con la federación de su identidad dentro de un dominio y en relación con el uso y la divulgación de información personal, así como facilitar determinadas interacciones entre proveedores de identidad, proveedores de servicios y proveedores de atributos sin divulgar la identidad del usuario.

Se incluyen las siguientes herramientas:

- Controles de acceso: las especificaciones de Liberty permiten a los proveedores tomar decisiones de control de acceso en nombre del usuario. Los proveedores tendrían que ofrecer un mecanismo por el cual el usuario pueda especificar su política de autorización (por ejemplo, podría no querer que su nombre fuese divulgado en una web de un diario, pero sí en la AP).
- Directivas de uso: las especificaciones de Liberty describen un contenedor que puede ser empleado para indicar o apuntar a directivas referidas al uso que se pretende para un atributo solicitado o el uso permitido para un atributo divulgado. El proveedor de atributos y el proveedor de servicio pueden negociar directivas de uso adecuadas, por ejemplo suministrando la lista de directivas aceptadas por el usuario, en caso de discrepancia.
- Identificadores opacos: las especificaciones de Liberty permiten el uso de identificadores opacos, que consisten en la asignación de una secuencia arbitraria de caracteres por el proveedor de identidad al usuario, que sólo tiene sentido en el contexto de una relación entre este proveedor de identidad y un proveedor de servicio concreto. Esta técnica ofusca la identidad del usuario y hace que sea mucho más difícil el seguimiento de las acciones del usuario en diferentes proveedores de servicios.

  Un identificador opaco permite a cada proveedor de servicio conocer qué usuarios con cuentas locales han navegado por su web, facilitando la federación de identidad entre los usuarios del proveedor de identidad y el proveedor de servicio sin transferir ninguna información personal sobre el usuario al proveedor de servicio antes de la federación.

- Protocolos de identidad anónima: las especificaciones de Liberty contienen protocolos para compartir datos de personalización con un proveedor de servicio de manera anónima, que permite ofrecer webs personalizadas sin ninguna divulgación de datos personales, empleando un identificador transitorio.

Finalmente, se ha publicado una especificación con cinco configuraciones de privacidad que indican las preferencias de los usuarios respecto al uso de sus datos personales, descritas en lenguaje natural y en lenguaje de preferencias de privacidad (W3C P3P):

- Privacidad estricta
- Privacidad con cautela
- Privacidad moderada
- Privacidad flexible
- Privacidad informal

Los trámites entre las empresas y la Administración. Casos de éxito

Emma Suevos i Guillamet
Directora de Calidad y Procedimientos de l'Agència Catalana de Certificació

1_INTRODUCCIÓN

B2G es la abreviatura del término inglés Business to Government y hace referencia a la optimización de los procesos de relación entre las empresas y la Administración Pública a través del uso de Internet.

Este concepto se aplica a las webs en las que los diferentes entes públicos (locales, autonómicos, estatales, etc.) ofrecen trámites electrónicos administrativos con el sector privado (proveedores de la Administración, empresas que deben liquidar impuestos, subvenciones, etc.).

En los últimos años se ha incrementado de manera muy notable este tipo de relaciones telemáticas, y se ha pasado de unas webs que sólo ofrecían información de interés para el mundo empresarial a un segundo estadio en el cual se ponía a disposición la descarga de los formularios de los trámites, y una tercera fase en la cual se permite la interacción telemática completa. Esta última es posible, principalmente, por el uso de la firma electrónica reconocida y al hecho que esta hace que el trámite telemático equivalga al efectuado presencialmente con firma manuscrita.

Hay que destacar el hecho de que cada vez se lleven a cabo más estrategias y proyectos sobre los trámites en los cuales hay más intensidad de interacción entre el sector público y las empresas, como puede ser la contratación pública, los registros públicos, la compra de bienes y servicios, etc.

Las empresas y los profesionales, por su parte, solicitan no tener que aportar ninguna documentación relativa a sus circunstancias que ya esté en poder de la Administración. Por esto es imprescindible extender a todas las administraciones diferentes medidas como las siguientes:

- La capacidad de emitir e intercambiar los certificados relativos a datos y situaciones de las empresas entre las administraciones, y entre los notarios y los diferentes registros.

- La implantación de mecanismos de reducción de la aportación de documentos por parte de las empresas, mediante el uso de la declaración responsable electrónica.
- La compulsa electrónica de documentos que estén almacenados en archivos públicos electrónicos y posteriormente intercambiados entre administraciones.

Por todo esto se ve que los procedimientos administrativos de acceso a información administrativa de manera telemática pueden ser más eficientes que los tradicionales y permiten nuevas aplicaciones, como el seguimiento posterior de los asuntos o la provisión de información bajo demanda y personalizada.

Hay que destacar que las administraciones tributarias son las que más han adelantado en la creación de sistemas organizados de uso de la firma electrónica, y lideran absolutamente los aspectos de pagos, facturas y declaraciones por vía telemática. Por este motivo sus modelos de organización pueden ser un referente para el resto de administraciones.

En este contexto hay que remarcar que no hay una visión de conjunto de los diferentes niveles de Administración Pública, puesto que podemos considerar que cada administración pública hace su propia apuesta sobre cómo llevar a cabo la tarea de impulsar las relaciones electrónicas con el mundo privado.

Aún así, es posible analizar varios casos de éxito en cuanto a la relación telemática empresas - Administración Pública. La información recogida en estas páginas muestra un buen panorama de múltiples iniciativas locales, autonómicas y estatales, que llevan a pensar que cada vez es más grande el interés desde el ámbito público de poner los medios para que las relaciones electrónicas con el tejido empresarial mejoren la eficacia y la eficiencia de los procedimientos administrativos por un lado, y de la inversión en tiempo y dinero por parte de las empresas, por otro.

En este capítulo queremos analizar iniciativas de diferentes niveles de administración territorial e institucional y sistematitzar bajo unos mismos parámetros informativos algunas de las iniciativas más exitosas llevadas a cabo para el impulso del B2G en los últimos tiempos.

Las áreas temáticas de las cuales se han seleccionado los proyectos que se exponen aquí han sido diversas: registros públicos, declaraciones,

contratación administrativa, pagos tributarios, consulta de información en poder de la Administración, etc. Aun así se trata de categorías que permiten comparar entre las diferentes iniciativas en las que más intensamente se sitúa el impulso de las relaciones electrónicas publicoprivadas.

Los proyectos que se exponen son los siguientes:

1. RELI del Departamento de Economía y Finanzas de la Generalitat de Cataluña
2. Tramitación telemática de Declaración del uso y la contaminación del agua de la Agencia Catalana del Agua
3. Plataforma de compras de las administraciones públicas de Localret
4. Tràmites municipales con empresas en la web del Ayuntamiento de Manresa
5. Carpeta de las empresas y entidades del Ayuntamiento de Barcelona
6. Oficina virtual para empresas y profesionales de la AEAT (Agencia Estatal de Administración Tributaria).

Optamos por recoger los parámetros comunes siguientes de cada uno de estos proyectos :

1. Nombre del proyecto
2. URL donde se encuentra
3. Fecha de inicio del proyecto
4. Breve descripción
5. Motivación de la necesidad / problema que intenta resolver
6. Objetivos
7. Público objetivo
8. Nombre de usuarios
9. Identificación de indicadores
    a) Número de transacciones realizadas
    b) Número de transacciones firmadas electrónicamente
    c) Otros que pueda tener el proyecto
10. Tipo de certificado digital con el que se hace el trámite
11. Evolución: nuevas funcionalidades que se prevé incorporar, etc.
12. Etc.

CASO 1: Registro Electrónico de Empresas Licitadoras (RELI) del Departamento de Economía y Finanzas de la Generalitat de Cataluña

1. Nombre del proyecto:
Registro Electrónico de Empresas Licitadoras (RELI)

2. URL donde se encuentra:
https://reli.gencat.net

3. Fecha de inicio del proyecto:
septiembre de 2005

4. Breve descripción:

La Junta Consultiva de Contratación Administrativa gestiona desde el año 1999 el Registro de Licitadores de la Generalitat de Cataluña. Este registro se creó para simplificar los trámites que deben seguir las empresas en los procedimientos de adjudicación de los contratos públicos. El Decreto 107/2005, de 31 de mayo, creó el RELI, que sustituye al anterior Registro. Este decreto introduce importantes modificaciones en el régimen de funcionamiento de este Registro, con la intención fundamental de hacerlo más útil y práctico para las empresas.

Las características esenciales del RELI son:

- **Voluntario:** no es necesario estar inscrito en el RELI para poder contactar con las administraciones públicas.
- **Gratuito:** la inscripción en el RELI no está sometida a ninguna tasa ni precio público.
- **Electrónico:** los datos que se incluyen en el RELI se introducen en formato electrónico.
- **De inscripción indefinida:** la inscripción en el RELI no está limitada en el tiempo.
- **De datos vigentes:** en el RELI únicamente constan datos vigentes de las empresas, con lo cual una vez formalizada la inscripción hay que actualizar los datos a medida que van variando.
- **Válido para las diferentes administraciones públicas:** las empresas inscritas en el RELI pueden participar tanto en procedimientos de licitación de la Administración de la Generalitat de Cataluña como en licitaciones de las diferentes entidades locales y de otras administra-

ciones públicas catalanas si así lo acuerdan y lo recogen, en este caso, los respectivos escritos.

- Incorpora información agregada de las diferentes empresas inscritas, con el fin de que los órganos y las mesas de contratación puedan disponer de información útil en los procesos de invitación y selección de Empresas en los procedimientos negociados por razón de cuantía y contratos menores.

5. Motivación de la necesidad / problema a resolver por el proyecto:

Las novedades esenciales que aporta el RELI respecto al anterior Registro son:

- **Formato electrónico:** no hace falta que las empresas inscritas en el RELI aporten, en los diferentes procedimientos de licitación, ningún certificado acreditativo de inscripción. Son los órganos de contratación y las mesas de contratación los que, de oficio, acceden por medios electrónicos de forma directa y segura a los datos contenidos en el Registro. Desaparece, por lo tanto, el certificado del Registro de Licitadores en formato papel. El procedimiento consiste en que la empresa puede indicar en el sobre su NIF y el del licitador y manifestar, si lo cree oportuno, mediante una declaración responsable, la vigencia de los datos inscritos en el RELI, indicando también el NIF de la empresa y el NIF y nombre de la persona apoderada que licita en su representación.

  También es importante destacar que el órgano o la mesa de contratación generan directamente el certificado, en formato electrónico, que se une al expediente administrativo.
- **Los órganos o las mesas de contratación** acceden de oficio a la base de datos del RELI para comprobar los correspondientes datos registrales de su empresa. En este sentido, si hace falta, los órganos de contratación o las mesas de contratación se ponen en contacto con la empresa licitadora en el supuesto de que se haya de enmendar o completar algún dato. En cualquier caso, los escritos de cláusulas administrativas de la licitación correspondiente hacen referencia a esta circunstancia.
- **Procedimiento de inscripción y de actualización de datos por vía telemática:** no hace falta rellenar y presentar la correspondiente soli-

citud en papel. Las empresas pueden formalizar y enviar por vía telemática la correspondiente solicitud desde sus oficinas.

- **Consulta de datos:** las empresas inscritas pueden consultar sus datos por Internet.
- **Seguridad:** todos los trámites telemáticos que hagan las empresas con el Registro se llevan a cabo con el máximo nivel de seguridad, a través de la firma electrónica reconocida, con idénticos efectos jurídicos que la firma manuscrita.
- **Incremento de la información del Registro:** el RELI incorpora datos de las empresas referidas a su solvencia económica financiera y técnica o profesional.

6. Objetivos:

El RELI es una evolución del Registro de Licitadores que tiene el objetivo principal de facilitar la concurrencia de las empresas en procedimientos de adjudicación de contratos públicos y aumentar significativamente la agilidad en la tramitación.

Por esto incorpora las nuevas tecnologías, para simplificar los trámites y ahorrar costes a las empresas y a las administraciones en los procedimientos de licitación.

Los objetivos principales son los siguientes:

- Los órganos y las mesas de contratación de las administraciones públicas pueden acceder, de oficio, de forma electrónica y segura a los datos registrales de las empresas inscritas.
- El RELI es depositario de los documentos que las empresas tienen que aportar en cada procedimiento de licitación, para acreditar la personalidad jurídica, la capacidad, la representación y la solvencia.
- El hecho de que el RELI permita presentar esta documentación una sola vez evita que esta se deba aportar en futuras licitaciones.
- Se quiere sustituir el grueso de papeles del sobre A en los procedimientos de adjudicación por la posibilidad de que los órganos y las mesas de contratación se conecten electrónicamente a los datos del RELI.
- Abre un nuevo canal de comunicación con las empresas y con otras administraciones públicas.

- Quiere contribuir a la penetración definitiva de las nuevas tecnologías en los procedimientos de contratación de las administraciones.
- Notificaciones electrónicas con idénticos efectos que las notificaciones en papel.
- Permite concentrar los esfuerzos en la preparación de la propuesta económica y técnica por parte de las empresas.

7. Público objetivo:

Se pueden inscribir en el RELI personas físicas, personas jurídicas, es decir, sociedades mercantiles, asociaciones, fundaciones, cooperativas, agrupaciones de interés económico y sociedades civiles particulares, y cualquier empresa o persona física extranjera, comunitaria o extracomunitaria entre otras, que estén constituidas legalmente.

8. Nombre de usuarios:

Actualmente hay 1.098 personas usuarias del sistema, que se dividen de la manera siguiente:

- Administración de la Generalitat de Cataluña: 395
- Organismos y empresas públicas: 289
- Entidades adheridas (entidades locales y otras administraciones): 414

9. Identificación de indicadores:

a) Número de certificados generados:
   - Año 2006: **2.538** en total, divididos en:
     - Departamentos de la Generalitat: 781
     - Sector público: 1.359
     - Entidades adheridas: 398
   - Año 2007 (a 30 de abril): **1.077** en total, divididos en:
     - Departamentos: 348
     - Sector público: 560
     - Entidades adheridas: 169

a) Número de Empresas inscritas (a 30 de abril):
   1.162 en total, divididas en:
   - Pequeña empresa: 406
   - Microempresa: 446

- Mediana empresa: 194
- No-pyme: 97
- Personas físicas: 19

10. **Tipos de certificado digital con los que se hace el trámite**: Todos los clasificados por CATCert.

11. **Evolución: nuevas funcionalidades que se prevé incorporar, etc.**

Incorporación de la firma electrónica de ficheros adjuntos al formulario de introducción de datos que firman las empresas mediante el Formsign.

Posibilidad de uso de la miniaplicación de firma de CATCert.

CASO 2: Tramitación telemática de Declaración del uso y la contaminación del agua (DUCA) de la Agencia Catalana del Agua (ACA)

1. **Nombre del proyecto:**

   e-DUCA (Declaración del uso y la contaminación del agua)

2. **URL donde se encuentra:**
   http://mediambient.gencat.net/aca/ca//tramitacions/canon/tramits/tramitacions.jsp

3. **Fecha de inicio del proyecto:**
   1 de abril de 2005

4. **Breve descripción:**

La ACA ha creado una aplicación para agilizar y facilitar la formalización de la DUCA.

e-DUCA es una aplicación que permite a los usuarios realizar la DUCA utilizando las mismas herramientas de cálculo que usa la ACA para determinar el canon del agua, especialmente la parte que corresponde al tipo de gravamen específico, su impresión en el formato de los modelos oficiales y la generación de un fichero que, una vez enviado a la ACA, permite la tramitación rápida de la DUCA. El fichero se puede enviar a través de la web de la ACA o bien por correo electrónico acompañado de la declaración impresa firmada y sellada en la que consta el nombre del fichero asociado.

Alternativamente, el fichero se puede enviar a la dirección de correo electrónico que aparece en la web indicando en el asunto la referencia **DUCA**

H0492. En este caso, para que la DUCA sea efectiva, hay que enviarla impresa, debidamente firmada y sellada.

La aplicación permite, entre otras cosas, copiar una declaración anterior para generar una nueva. Este hecho simplifica mucho la tarea de generación de la DUCA cuando se trata de sujetos con pocos cambios en su actividad durante el período comprendido entre una declaración y otra.

La aplicación trabaja con las tarifas vigentes en el momento de la instalación. Por lo tanto, si se produce cualquier cambio, hay que actualizar los datos conectándose a la web de la ACA. También se pueden encontrar otras actualizaciones de tablas (municipios, depuradoras, etc.) y mejoras de la aplicación.

La presentación telemática de la DUCA y B6, con firma electrónica basada en identificación de usuario y palabra de paso, requiere ejecutar el procedimiento de seguridad siguiente para cada presentación:

1. Inicio de la sesión de trabajo por parte del presentador. Se genera un dato que identifica esta sesión. Se graba la fecha y la hora del inicio de sesión. Se empiezan a grabar todas las acciones del presentador en el registro del servidor web y de la aplicación accedida.
2. Solicitud de identificación del presentador, mediante credencial generada de acuerdo con la política de identificación y autenticación indicada en la sección y remisión al sistema de presentación mediante un canal protegido, de acuerdo con la política de cifraje de comunicaciones indicada en la sección de este documento.
3. Verificación de la identificación. Se devuelve un mensaje interno que indica el éxito de la verificación, que se graba en el registro del servidor web o de la aplicación, según convenga.
4. Introducción de los datos o documentación que hay que presentar, que se graban en el aplicación, para producir posteriormente el documento. La remisión de los datos o de los documentos también se graba en el servidor web.
5. Verificación de los datos que hay que presentar y manifestación de la voluntad de presentar. Aparece una pantalla con todos los datos

aportados y con el mensaje de confirmación que garantiza la manifestación de voluntad, de acuerdo con la política de desarrollo del software indicada en la sección de este documento.

6. Generación de la evidencia forense sobre los datos grabados anteriormente, de acuerdo con la política de desarrollo del software indicada en la sección de este documento.
7. Firma del documento de presentación de la DUCA y B6 y de la evidencia forense generada, de acuerdo con la política de firma electrónica indicada en la sección de este documento.
8. Remisión al Registro interno y producción del recibo de confirmación correspondiente, de acuerdo con la política de firma electrónica indicada en la sección de este documento.

5. Motivación de la necesidad / problema a resolver por el proyecto:

La aplicación permite agilizar el trámite y hacerlo más fácil para el usuario. Evita la remisión de modelos en papel con la demora que esto comporta. Entra dentro del proceso de modernización de la ACA y de adaptación al proyecto de administración electrónica.

6. Objetivos:

La tramitación vía web se debe hacer en la dirección http://mediambient.gencat.net/aca/ca/tramitacions/canon/tramits/tramitacions.jsp, y sustituye totalmente la tramitación en papel.

De acuerdo con el artículo 13 del Decreto 324/2001, de 4 de diciembre, relativo a las relaciones entre la ciudadanía y la Administración de la Generalitat de Cataluña a través de Internet, el documento de presentación de la DUCA y B6 tendrá los mismos efectos que si hubiera sido presentado y firmado en soporte papel.

7. Público objetivo:

Esta aplicación está dirigida a todos los sujetos susceptibles de presentar la DUCA y a todos los que disponen de suministro de agua para fuentes propias y que deben declarar trimestralmente las lecturas de los contadores.

El número de usuarios potenciales es de 5.800 aproximadamente.

8. **Número de usuarios:**
   Actualmente se conectan unos 2.300 usuarios.
9. **Identificación de indicadores:**

- **Número de transacciones realizadas:** aproximadamente 16.500.
- **Número de transacciones firmadas electrónicamente:** todas se firman, por lo tanto, 16.500.

10. **Tipo de certificado digital con el que se hace el trámite:**

Con respecto al usuario, el trámite se hace con firma electrónica ordinaria, es decir, con el código de usuario y la contraseña que suministra la ACA. También se puede utilizar un certificado digital.

La firma del documento de presentación de la DUCA y B6 se debe basar en un certificado de dispositivo de aplicación digitalmente asegurada de clase 1 (CDA-1) emitido a la ACA por la entidad de certificación EC-SAFP, de la jerarquía de la Agencia Catalana de Certificación.

11. **Evolución: nuevas funcionalidades que se prevé incorporar, etc.**

Se han de llevar a cabo las adaptaciones necesarias que estén determinadas por cambios legales en la materia.

CASO 3: Plataforma de compras de las administraciones públicas de Localret

1. **Nombre del proyecto:**
PECAP (Plataforma electrónica de contratación de las administraciones públicas)

2. **URL donde se encuentra:**
http://www.pecap.org

3. **Fecha de inicio del proyecto:**
1 de enero de 2005

4. **Breve descripción:**

La Plataforma Electrónica de Contratación es un portal de Internet que permite a los entes locales y al resto de administraciones públicas llevar a cabo, por vía telemática, determinadas fases de la contratación administrativa de suministros, obras y/o servicios.

Esta Plataforma, dado el marco legal actual, permite hacer contratos menores y determinados trámites de los contratos de suministro, obras y servicios que se adjudiquen mediante el procedimiento negociado sin publicidad.

En la práctica, según la legislación actual, permite hacer los trámites siguientes:

- Contratos menores de suministros y servicios: cuando la cuantía no exceda los 12.020,24 €.
- Contratos menores de suministros de bienes consumibles: cuando la cuantía no exceda los 60.101,21 €.
- Contratos menores de obras: cuando la cuantía no exceda los 30.050,61€.
- Contratos mediante procedimiento negociado de suministros y servicios: los bienes son de cuantía inferior a 30.050,61€.
- Contratos mediante procedimiento negociado de obras: de cuantía inferior a 60.101,21€.
- Negociaciones sobre productos o servicios homologados previamente, sin ningún límite económico.

La PECAP proporciona a las administraciones públicas un amplio directorio de proveedores y permite efectuar electrónicamente tres acciones de compra:

- La compra por catálogo.
- La solicitud de presupuestos o gestión de ofertas.
- La subasta o negociación en línea.

La Plataforma está basada en los principios siguientes:

- Autenticidad (identificación y competencia).
- Confidencialidad.
- Integridad (y también el no-rechazo).
- Conservación.
- Disponibilidad.
- Publicidad.
- Flexibilidad (adaptación a los cambios y a las mejoras tecnológicas).

Para utilizar la PECAP hay que disponer de certificado digital.

La PECAP proporciona tres funciones básicas:

- Un amplio directorio de proveedores para facilitar la competitividad en los procesos de compra.
- La compra de productos o servicios mediante la convocatoria de negociaciones en línea y/o peticiones de presupuesto.

La compra de productos o servicios a través de los catálogos electrónicos publicados en la Plataforma por parte de los proveedores del mercado.

5. Motivación de la necesidad / problema a resolver por el proyecto:

PECAP.org es un servicio que ofrece Localret a sus asociados y a otras administraciones públicas, como respuesta a un mandato de la asamblea general del Consorcio del año 2000.

Al mismo tiempo, este servicio refuerza el compromiso de Localret con el proyecto Administración Abierta de Cataluña (AOC) y concreta el compromiso de todas las fuerzas políticas catalanas representadas en el Parlamento de Cataluña y de los ayuntamientos, representados por el Consorcio, para facilitar la contratación de bienes y de servicios de la administración pública catalana, optimizando los recursos públicos. Se encuentra explícito en el acuerdo parlamentario de 23 de julio de 2001: el Pacto para la promoción y el desarrollo de la sociedad de la información en las administraciones públicas catalanas.

La creación de la Plataforma persigue modernizar y digitalizar las administraciones públicas, aplicar innovación para mejorar la eficiencia (modernización y simplificación), extender el uso de los elementos de seguridad (técnica y jurídica) en las transacciones en línea y socializar las empresas y las administraciones en el uso de los certificados digitales y la firma electrónica.

¿Para qué sirve?

Administraciones públicas

- Las administraciones públicas pueden buscar productos o servicios o proveedores en las condiciones más ventajosas.
- Las administraciones públicas pueden publicar telemáticamente anuncios de ofertas u ofertas de contratos, de una manera persona-

lizada a una determinada empresa o a más de una, o bien a una pluralidad indeterminada de éstas.

- Los entes pueden acceder a la web de los proveedores de que dispongan y conocer sus productos, servicios y precios.
- Los entes pueden recibir de los proveedores, por correo electrónico, las novedades y las actualizaciones de sus productos y servicios, y sus catálogos digitales.
- Los entes pueden constituir una comunidad virtual de agentes responsables de la contratación que les permita intercambiar información, conocimientos, documentación y experiencias.

Proveedores

- Ofrecer productos o servicios en las condiciones más óptimas.
- Figurar en el directorio de empresas del mercado, donde aparecerá su empresa caracterizada por el tipo de actividad que lleva a cabo, de modo que las diferentes administraciones públicas que hay en el mercado lo puedan invitar a participar en sus procesos de contratación.
- Crear y gestionar su propio catálogo electrónico de venta de productos, que será visible y accesible para todas las administraciones públicas que hay en el mercado, o bien crear y gestionar un catálogo específico para una administración pública determinada.
- Participar en las peticiones de información, precio o propuesta, y subastas de compra que convocan las diferentes administraciones públicas, a las que sea invitado o a las que su empresa considere interesantes y estén abiertas a cualquier miembro del mercado.
- Ofrecer sus productos y servicios, así como sus precios, desde su web.
- Hacer llegar a las administraciones públicas, por correo electrónico, las novedades y las actualizaciones de sus productos y servicios, y sus catálogos digitales.

Ventajas

- La Plataforma Electrónica de Contratación simplifica los procesos de contratación.
- Permite reducir la duración de los procesos de negociación.

- Facilita la integración los procesos de contratación con diferentes procesos internos de las administraciones públicas y de los proveedores.
- Reduce el volumen de papel empleado en los expedientes de contratación.
- Permite operar comercialmente en un entorno seguro, transparente y neutral, y se puede operar las 24 horas del día, los 365 días del año.
- Ofrece un mercado al que pueden acceder nuevos clientes, en este caso, administraciones públicas.

Valores

- El incremento de la transparencia en los procesos de contratación.
- El acceso a una mayor masa crítica de empresas y proveedores y de administraciones públicas contratantes.
- El acceso a unos precios de mercado más óptimos.
- Un nuevo canal de acceso al mercado para encontrar proveedores, productos o servicios.
- Transparencia hacia el mercado en todos los procesos.
- Optimización de precios de productos y servicios.
- Facilidad de comparación de ofertas de los diferentes proveedores.
- Simplificación del proceso de compra y reducción de tiempo tanto de la negociación como de la petición.
- Facilidad para establecer políticas corporativas de compra.
- Disminución de volumen de papel que se debe gestionar en las compras.
- Para las administraciones, la plataforma no representa ningún coste.

6. Objetivos:

El objetivo principal es mejorar la eficiencia operativa y la productividad en la gestión de las compras.

La PECAP facilita la comunicación y la transmisión de información entre las administraciones públicas y las empresas. Proporciona a las administraciones públicas un amplio directorio de proveedores y permite efectuar electrónicamente tres acciones de compra:

- La compra por catálogo
- La solicitud de presupuesto o gestión de ofertas
- La subasta o negociación en línea.

La Comisión Europea ha hecho constar en el Plan de acción de la CoE sobre los contratos públicos electrónicos que, si se generaliza la contratación en línea, las administraciones públicas ahorrarán entre el 50 % y el 80 % del coste de las operaciones.

Por eso la PECAP representa:

- Nuevo canal de acceso al mercado para encontrar proveedores, productos o servicios.
- Transparencia.
- Incrementar la competencia y la eficiencia en los mercados de contratación pública.
- Facilitar la comparación de ofertas.
- Simplificar el proceso de compra y reducir el tiempo de la negociación y de las peticiones de oferta.
- Facilitar el establecimiento de políticas corporativas de compra.
- Familiarizar a las administraciones públicas y a las empresas privadas con el nuevo marco jurídico de la contratación pública electrónica en Europa, con los nuevos medios electrónicos de compra y los nuevos procedimientos de contratación.

En definitiva, mejorar dentro de lo posible la gestión en las administraciones públicas y, consecuentemente, posibilitar una mayor disponibilidad de recursos para dedicarlos directamente a nuevos servicios dirigidos a la ciudadanía.

7. Público objetivo:

La PECAP va dirigida a todas las administraciones públicas, especialmente a las entidades que integran la administración local catalana, la Generalitat de Cataluña, los organismos autónomos y las entidades de derecho público con personalidad jurídica propia, vinculadas o dependientes de cualquiera de las administraciones públicas catalanas.

Por otro lado, se dirige a todas las empresas interesadas en contratar con las administraciones públicas catalanas.

8. Número de usuarios:

Hay 95 empresas y 99 administraciones públicas adheridas a la PECAP, que se dividen en:

- 9 consejos comarcales.
- 87 ayuntamientos.
- 2 universidades.
- 1 otros.

9. Identificación de indicadores:

a) **Número de transacciones llevadas a cabo durante el año 2006:**

– Peticiones de presupuesto (RFQ): 17.

– Subastas o negociacions en línea: 42.

b) **Número de transacciones firmadas electrónicamente:** todas las acciones requieren el uso de certificado digital

c) **Otros que pueda tener el proyeto:**

– Volumen de las subastas el año 2006: 2.055.560,42 €.

– Ahorro del 16%: 326.248,76 €.

10. Tipo de certificado digital con el que se hace el trámite:

- **Administraciones públicas:** certificados digitales de CATCert.
- **Empresas:** certificado digital en software de Camerfirma.

Proveedores de certificados de firma electrónica:

- **Camerfirma:** autoridad de certificación de las cámaras de comercio, proveedora de certificados de firma electrónica a las empresas.
- **Agencia Catalana de Certificación:** entidad prestadora de servicios de firma electrónica de las administraciones catalanas.

11. Evolución: nuevas funcionalidades que se prevé incorporar, etc.

En referencia a las mejoras que se tienen planificadas en la PECAP:

- Mejora de la información posterior (proveedores invitados: nombre, NIF, dirección, etc.; ofertas: hora, importe, etc.) para transportarla al expediente papel y para transportarla a un expediente electrónico.

- Permitir grabar toda la subasta para poderla visualizar a posteriori.
- Mejorar el diseño de las gráficas.
- Permitir alternar el seguimiento de varias líneas de subasta.
- Incorporar un paro automático: aviso automático cuando se esté produciendo una incidencia.
- Que, por defecto, la subasta no admita precios peores, sino que sólo sea posible mejorar las ofertas anteriores.
- Integrar la PECAP en el servicio de validación de PSIS (Plataforma de servicios de identificación y firma) de CATCert.
- Incorporar el sello de fecha y hora al cierre de la subasta: la TSA (autoridad de sellado de tiempo) de CATCert.
- Acceso al RELI y al catálogo de bienes homologados de la Generalitat.
- Facturación electrónica.

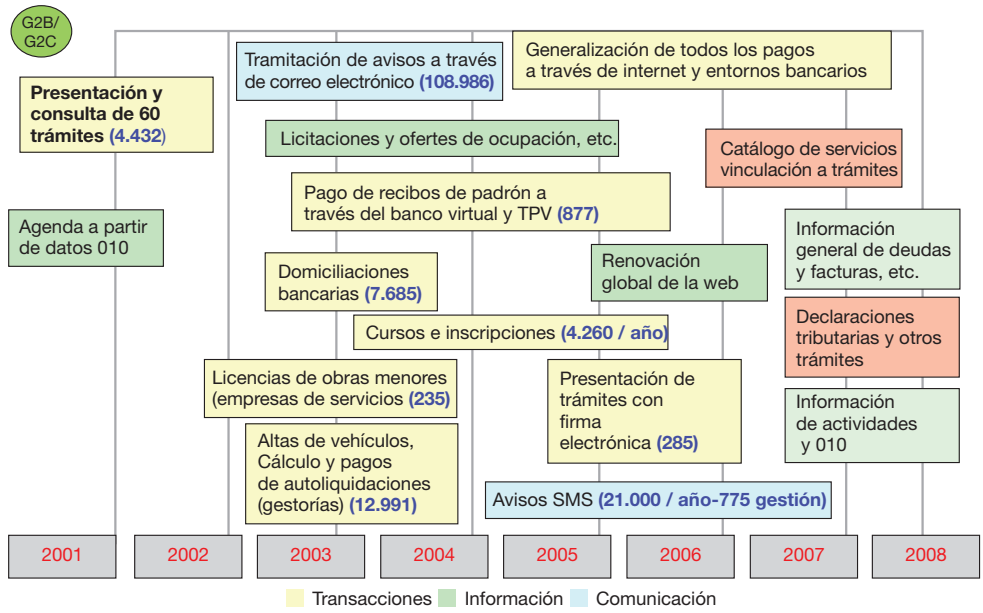
CASO 4: Trámites municipales con empresas en la web del Ayuntamiento de Manresa

1. **Nombre del proyecto:**
   Trámites a través de Internet.
2. **URL donde se encuentra:** https://www.ajmanresa.cat/php/tramits
3. **Fecha de inicio del proyecto:**
   15 de octubre de 2002
4. **Breve descripción:**

Si entendemos por administración electrónica el conjunto de actuaciones orientadas a mejorar la gestión de la Administración, la participación y la prestación de servicios públicos a través de las TIC, uno de los principales ámbitos es el *front-office* (G2B/G2C), es decir, las acciones necesarias para conseguir que, de forma progresiva y segura, el ciudadano y las empresas puedan llevar a término la mayor parte de trámites municipales a través de Internet. Por eso ya hay 24 trámites que se realizan con certificado digital, entre los cuales destacan las comunicaciones previas de obras, las licencias de apertura de establecimientos y multas y alegaciones.

En este contexto, además de facilitar información de gestión y comunicaciones electrónicas (correo electrónico, SMS), se llevan a cabo

proyectos orientados a realizar la transacción completa. Entre estos últimos destacan los siguientes:



Tanto los trámites como los pagos que se llevan a término en la web, se integran automáticamente vía servicios web en la gestión interna de procedimientos y de recaudación respectivamente. Aun así, el sistema permite consultar el estado de resolución de los trámites presentados.

5. Motivación de la necesidad / problema a resolver por el proyecto:

En todos los proyectos de administración electrónica que está implementando el Ayuntamiento de Manresa la motivación principal es mejorar el servicio a las empresas y los ciudadanos, y evitar que deban desplazarse para hacer trámites con la administración municipal.

Concretamente, la declaración tributaria de altas de vehículos y el pago de la autoliquidación correspondiente, implicaba el desplazamiento diario de personal de gestorías al Ayuntamiento.

6. Objetivos:

A partir de la experiencia de las acciones realizadas, el Ayuntamiento trata de avanzar ampliando y consolidando los trámites en Internet hasta conseguir que cualquier gestión con la Administración se pueda hacer de forma no presencial.

7. Público objetivo:

Gestorías, colegios profesionales, empresas y ciudadanos en general.

8. Número de usuarios:

Para el proyecto de gestorías, el número de usuarios que se identifican es de 29. Se dispone de convenios con el Colegio de Arquitectos y con el Colegio de Abogados.

9. Identificación de indicadores:

	Anteriores	2003	2004	2005	2006	Total
Declaraciones tributarias (cálculo y pago) (gest.)	566	2.539	2.919	3.504	3.463	12.991
Presentación de trámites	601	560	760	612	1.899	4.432
Domiciliaciones bancarieas	1.009	1.360	1.262	1.614	2.440	7.685
Pagos de recibos y liquidaciones				242	635	877
Cursos e inscripciones (inscripción y pago)			3.800	4.100	4.260	12.160
Total	**2.176**	**4.459**	**8.741**	**10.072**	**12.697**	**38.145**

10. Tipos de certificados digitales con los que se hace el trámite:

todos los clasificados por CATCert.

11. Evolución: nuevas funcionalidades que se prevé incorporar:

- Ampliar el número de declaraciones tributarias que tienen que utilizar prioritariamente las gestorías.
- Convenio con la AOC para llevar a cabo notificaciones telemáticas.
- Mejorar la funcionalidad de los trámites en Internet vinculándolos al catálogo de servicios y haciendo uso de la busca semántica.
- Ampliar el número de trámites.

CASO 5: Carpeta de las empresas y entidades del Ayuntamiento de Barcelona

1. Nombre del proyecto:

Carpeta de las empresas y entidades

2. URL donde se encuentra:

www.bcn.es/carpeta-empreses

3. Fecha de inicio del proyecto:
junio de 2005

4. Breve descripción:
Este servicio proporciona información de los datos fiscales de la empresa o entidad para que puedan hacer más ágiles las gestiones con el Ayuntamiento. También da información de interés general para las empresas.

Siguiendo la arquitectura de la nueva plataforma iNet del Ayuntamiento de Barcelona, basada en J2EE, la Carpeta de las empresas es un servicio de agregación de la información de que dispone el Ayuntamiento sobre una empresa. Esta agregación es posible gracias a la implantación del modelo de información de base que identifica unívocamente cualquier información de cariz fiscal con un ciudadano.

Funcionalidades y estructura de la información

La información disponible está agrupada en diferentes menús accesibles desde la página de inicio del servicio una vez que el usuario se ha identificado y ha accedido a los datos de la empresa. La información disponible es:

- **Datos fiscales:** razón social, NIF, teléfono y direcciones (fiscal, electrónica y de notificación). El servicio expone a la vez la relación de trámites relacionados que pueden ser de interés en este punto. Entre otros: la modificación de errores en nombre, apellidos y direcciones, y cambios en las direcciones fiscales o de notificación.
- **Objetos fiscales:** inmuebles, vehículos, IAE, residuos y vados. Se muestran los objetos fiscales de la empresa –inmuebles, vehículos, IAE, residuos y vados– con sus identificadores y las referencias asociadas, por ejemplo: dirección, referencia y valor catastral para inmuebles, identificador y matrícula para vehículos, período de liquidación de la IAE, etc. También se exponen los trámites relacionados, como por ejemplo la domiciliación bancaria de tributos, la autoliquidación de plusvalía, alegaciones o recursos y cambios de titularidad.
- **Estado de los impuestos (pagados y pendientes):** relación de los tributos municipales y el estado de estos para la empresa contribuyente y, a la vez, acceso al trámite relacionado de obtención del certificado de pago de tributos municipal.

- **Estado de las multas (pagadas y pendientes):** relación de las multas pagadas y pendientes identificadas por el expediente, hecho denunciado, importe, fecha de infracción y/o de pago, si procede. Acceso al trámite relacionado de obtención del certificado de pago de tributos municipal.
- **Otras funcionalidades:** archivos generados y calendario del contribuyente: la funcionalidad de los archivos generados permite descargar en diferentes formatos –.pdf (Acrobat) o en archivo .xls MS Office (Excel)– las listas solicitadas por el usuario. La funcionalidad del calendario del contribuyente permite asociar avisos a los diferentes hitos fiscales.

5. Motivación de la necesidad / problema a resolver por el proyecto:

Tras el éxito de la Carpeta del Ciudadano, que entró en funcionamiento en marzo de 2004, el Ayuntamiento de Barcelona ha impulsado una iniciativa nueva que facilita que las empresas y las entidades lleven a cabo las gestiones relacionadas con la administración local por Internet.

La Carpeta de las Empresas y Entidades nace para facilitar el acceso de las empresas a sus datos fiscales con facilidad y rapidez. Las empresas, cada vez más, hacen las gestiones con sus proveedores y clientes por Internet.

La nueva herramienta se ha diseñado para permitir a las empresas, a las entidades y a los profesionales consultar y gestionar desde la página <**www.bcn.es/carpeta-empreses**> sus datos fiscales, los objetos fiscales, los impuestos pagados o pendientes de pago, la consulta sobre el estado de las multas y generar archivos que faciliten la gestión tributaria de estos colectivos y que ofrezca, a la vez, la relación de trámites asociados con estas actividades. Además, también se pueden visualizar las fechas de los próximos pagos gracias al calendario del contribuyente y al servicio de avisos asociado.

6. Objetivos:

La puesta en funcionamiento de la Carpeta de las Empresas y Entidades representa un gran paso cualitativo en la mejora de los servicios municipales que se ofrecen a través de Internet. Además, es un gran paso que abre las puertas a aplicaciones posteriores y nuevas que deben facilitar la relación entre las empresas y la administración local a la hora de hacer las gestiones administrativas.

El objetivo y la voluntad del Ayuntamiento de Barcelona es que, con un certificado digital de persona jurídica, las empresas puedan acceder a cualquier servicio que requiera su identificación.

La implantación efectiva de la administración electrónica en el Ayuntamiento de Barcelona es uno de los objetivos del gobierno municipal en el mandato 2003-2007, contenido en el Plan de actuación municipal y desarrollado por dos medidas de Gobierno, de abril de 2004 y de diciembre de 2005.

El objetivo es que los ciudadanos, las empresas y los profesionales se puedan relacionar con la administración municipal con toda normalidad, validez y seguridad jurídica a través de los medios electrónicos, especialmente Internet, para obtener información, realizar consultas, presentar reclamaciones, obtener certificados, hacer trámites y procedimientos y cualquier otro derecho que le reconozca el Derecho administrativo.

Dentro de este marco, el Ayuntamiento de Barcelona ha desarrollado, por un lado, un texto jurídico que le permita conseguir los objetivos planteados, es decir, la Ordenanza de administración electrónica, y, por otro, el desarrollo de las infraestructuras y herramientas necesarias para ejecutar una administración electrónica. En este último capítulo se incluye la Carpeta de las empresas.

7. Público objetivo:

Empresas, profesionales y entidades con domicilio fiscal en Barcelona.

8. Número de usuarios:

Actualmente unos 5.000.

9. Identificación de indicadores:

Número de transacciones realizadas: 7.500.

10. Tipo de certificado digital con el que se hace el trámite:

Para acceder, las empresas, entidades, universidades, fundaciones, asociaciones y los trabajadores autónomos necesitan un certificado digital de persona jurídica o de profesional emitido por una entidad certificadora reconocida y validada por el CATCert. A través de este identificador único, la Carpeta de las empresas y entidades agrega información y se configura como el punto de partida para las gestiones de las empresas con el Ayuntamiento.

11. Evolución: nuevas funcionalidades que se prevé incorporar, etc.

Enriquecer la oferta de tramitación integrada en la Carpeta.

CASO 6: Oficina virtual para empresas y profesionales de la AEAT. Presentación del impuesto especial sobre determinados medios de transporte (MODELO 576)

1. Nombre del proyecto:

IEDMT (impuesto especial sobre determinados medios de transporte)

2. URL donde se encuentra:

http://www.aeat.es

Inicio > Campañas > Impuesto especial sobre determinados medios de transporte

3. Fecha de inicio del proyecto:

Se inició el 1 de septiembre de 2005 para utilizarlo de forma voluntaria y desde el 1 de enero de 2006 es obligatorio por Internet.

4. Breve descripción:

Se habilita la presentación telemática del impuesto de matriculación, modelo 576, para los casos que estén exentos o no sujetos, según la Orden EHA/1981/2005 (BOE 20/06/2005).

Se debe presentar esta declaración-autoliquidación previamente a la matriculación del vehículo, embarcación o aeronave, e indicar las características. Generalmente se debe pagar y obtener un NRC (número de referencia completo) como justificante de pago.

Para evitar pagos duplicados se ha incorporado el número de bastidor en la solicitud de pago en la entidad financiera y se ha incrementado el control sobre la anulación del NRC.

Se genera un código electrónico que agiliza la matriculación en la Dirección General de Tráfico, la Marina Mercante y Aviación Civil.

5. Motivación de la necesidad / problema a resolver por el proyecto:

Facilitar la declaración del impuesto y mejorar el control de los importes declarados por los vehículos, reduciendo así los grados fiscales.

Además, desde la Dirección General de Tráfico se puede comprobar, mediante el código electrónico, que previamente se ha presentado la declaración a la AEAT.

6. Público objetivo:

El destinatario final del servicio es el comprador del vehículo, pero en la mayoría de casos el trámite lo realizan intermediarios, que generalmente son los concesionarios de vehículos en condición de colaboradores sociales.

7. Número de usuarios:

Varias decenas de millar, entre las personas que lo presentan en nombre propio y las que lo presentan en nombre de terceros.

8. Identificación de indicadores

- **Número de transacciones realizadas:**

Año	Transacciones
2005	20.885
2006	1.646.597
2007*	679.590

*Hasta el 6 de junio de 2007.

Además, se hacen transacciones adicionales para comprobar el número de justificante, la consulta íntegra y la modificación del número de bastidor.

- **Número de transacciones firmadas electrónicamente:**

Todas las presentaciones del modelo 576 se reciben firmadas electrónicamente.

9. Tipo de certificado digital con el cual se hace el trámite:

Certificados X.509 v3, generalmente en software de la Autoridad Certificadora FNMT Clase 2 CA y, en menor grado, por otras entidades de certificación admitidas para relacionarse con la AEAT según la Orden HAC/1181/2003 (BOE 15/05/2003).

En el caso del modelo 576 se han utilizado certificados de hasta 13 entidades de certificación diferentes.

10. Evolución: nuevas funcionalidades que se prevé incorporar, etc.

Se esperan cambios en los datos que se solicitan en la declaración y mejoras en el intercambio de información con la Dirección General de Tráfico.

Finalmente, queremos agradecer el apoyo recibido de los responsables de las iniciativas analizadas en este estudio, que en algunos de los casos nos facilitaron informaciones complementarias sobre sus actividades.

Lo que necesita una empresa para hacer trámites con las administraciones públicas

Jordi Masías
Director de CATCert

1_SITUACIÓN HISTÓRICA

Hasta ahora, las empresas se han relacionado con las administraciones públicas por diferentes cuestiones:

- Presentar alguna documentación o trámite: constitución, actualización de la información, etc.
- Hacer alguna inscripción en algún registro.
- Presentar alguna declaración.
- Presentar alguna encuesta.
- Ser proveedores de las administraciones públicas, etc.

Estas relaciones eran siempre presenciales y, por lo tanto, hacía falta desplazar a alguien en horario de oficina para poder efectuar la tramitación.

Algunas administraciones habían empezado a facilitar a las empresas estas gestiones, y habían puesto en marcha servicios de atención telefónica en los que se podía iniciar algún trámite, consultar ciertas informaciones, etc. También muchas habían empezado a facilitar a las empresas información sobre trámites a través de Internet. Pero, en todos los casos, finalmente era necesaria una presencia física ante la Administración, dado que se tenía que firmar algún papel, presentar alguna documentación, etc.

Con la modernización de la Administración se está dando un paso muy importante para que esta relación se pueda establecer telemáticamente y sea completa. Es decir, que no haga falta la presencia física en ninguna parte del procedimiento administrativo, y que, además, se pueda hacer las 24 horas del día. Esto permite mayor flexibilidad, pero sobre todo más eficiencia y, por lo tanto, menos costes.

Implica un esfuerzo muy importante por parte de las administraciones públicas, puesto que han de ir automatizando todos los procesos, no

sólo desde el punto de vista de la atención al ciudadano/empresario, sino sobre todo con respecto a los procesos internos de gestión de expedientes, que ahora no están en papel sino en formato electrónico.

La modernización de la Administración implica, entre otras cuestiones y como elemento muy importante, pasar de un formato papel a uno electrónico, pero no como hasta ahora, que sólo se trataba de un proceso de optimización de los trabajos de gestión interna, sino que el formato electrónico, mediante la firma electrónica, tiene ahora toda la validez jurídica. Por lo tanto, el formato electrónico se convierte en el formato en el cual se debe conservar el expediente a lo largo del tiempo.

Este hecho comporta cambios muy importantes dentro de la Administración: se debe dotar de herramientas de identidad digital y de firma electrónica, tal y como se ha explicado en capítulos anteriores, debe poner en marcha servicios como los registros telemáticos, notificaciones telemáticas, etc., y ha de implementar procesos internos de gestión electrónica de documentos y expedientes, hasta llegar al final, cuando hay que conservar los documentos electrónicos a lo largo del tiempo.

Todas estas tareas son similares a las tareas que están emprendiendo muchas empresas que también viven un proceso de modernización, tanto interno como en las relaciones con los clientes y proveedores, pero con la diferencia de que en el sector público la validez jurídica de los diferentes actos es un elemento clave en todo este proceso de modernización.

Por lo tanto, es evidente que las administraciones tienen un trabajo y un reto importante ante ellos y trabajan en esta dirección, pero también necesitan que los ciudadanos/empresas con quien se relacionen dispongan de determinadas herramientas imprescindibles para poder garantizar jurídicamente la seguridad de estas relaciones, y muy especialmente la validez jurídica del expediente administrativo electrónico.

2_EL FUTURO DE LA ADMINISTRACIÓN ELECTRÓNICA

Desde las administraciones públicas pensamos que la modernización ha de ir ligada a un uso muy intensivo de las tecnologías de la información y de Internet. No porque pensemos que el uso de las tecnologías de la información deben cambiar la Administración, sino porque no se puede

plantear una modernización y una mejor eficiencia de le Administración sin el uso de estas tecnologías.

Tal y como hemos visto, la seguridad, en general, y la identidad digital y la firma electrónica, en particular, son piezas clave en el impulso de la modernización de la Administración. Con estas herramientas, las administraciones públicas dan un paso adelante en la puesta en marcha de trámites a través de la red. Las garantías jurídicas necesarias para que las administraciones públicas puedan ofrecer a través de Internet los mismos servicios que hasta ahora ofrecían presencialmente, sólo se dan si estas herramientas las utilizan no sólo las administraciones públicas, sino también, y sobre todo, las empresas.

Muchas veces se ha hablado de que la futura Administración pública debe ser multicanal. Esto quiere decir que un ciudadano podrá acceder desde diferentes canales: presencial, teléfono, Internet, TDT, etc.

Si analizamos los diferentes canales y los tenemos en cuenta desde el punto de vista de las empresas, llegaremos rápidamente a la conclusión de que los canales más útiles son dos: teléfono e Internet. Hoy se nos hace difícil imaginar la TDT como canal útil para las empresas, aunque en un futuro, esperamos que próximo, sí que lo será para los ciudadanos. Con respecto al canal presencial, pensamos que para las empresas acabará siendo un canal auxiliar y cada vez menos utilizado.

Respecto al teléfono, pensamos que es un buen canal y que lo continuará siendo para obtener información, para iniciar algunos trámites, pero que hasta que no se puedan poner medios de autenticación seguros legalmente, difícilmente será un canal completo para hacer todas las transacciones. De todas maneras, empezamos a encontrar herramientas que nos van permitiendo incluir sistemas de identificación digital e, incluso, de firma electrónica en el teléfono móvil (más PDA que teléfonos), pero la utilización todavía es muy baja.

Finalmente, y en cuanto a Internet, pensamos que empieza a ser, y ha de acabar siendo, el canal básico de comunicación y de transacción de la empresa con la Administración pública, dado que permite la interactividad, unos niveles de seguridad adecuados, un acceso de 24 horas, 7 días a la semana y la inmediatez, pero, sobre todo, permite una cuestión clave para la empresa, la automatización.

Las empresas se relacionan con las administraciones públicas de dos modos: puntual o continuamente. En el futuro más inmediato vemos que para las que necesitan trámites puntuales, Internet es un buen medio, puesto que tiene todas las ventajas mencionadas antes. Pero los que tienen una relación más continuada encontrarán todavía más ventajas, puesto que Internet permite una comunicación entre ordenadores, es decir, se pueden automatizar algunos procesos para bajar considerablemente los costes, por ejemplo, los procesos de facturación telemática entre los proveedores y las administraciones.

3_LO QUE DEBERÍA TENER UNA EMPRESA PARA OPTIMIZAR LAS RELACIONES CON LAS ADMINISTRACIONES PÚBLICAS

Tal y como se ha comentado en este libro, el uso de Internet en las relaciones con garantías jurídicas y la validez del documento electrónico, hace que sea necesario incorporar un conjunto de herramientas y elementos en los dos extremos de la comunicación.

En el caso que nos ocupa, las relaciones entre la empresa y la Administración, nos encontramos con diferentes modelos:

Relación persona/servidor. Este es el caso en que una persona dentro de una empresa se relaciona con la Administración. Es el caso más habitual y, por lo tanto, el primero a considerar. En este caso hace falta que esta persona pueda acreditar todo un conjunto de cosas para poder garantizar la validez jurídica del acto:

- **La identidad.** Hace falta que esta persona disponga de una identidad digital que le permita identificarse ante la Administración como tal. Este es uno de los principios que hasta ahora se han garantizando a través de la presentación del DNI o del pasaporte. Tal y como se ha dicho en este libro, la forma más fiable con validez jurídica y de más futuro es utilizar un certificado digital, ya sea el DNI electrónico, el idCAT o, en el caso empresarial, los certificados digitales de CAMERFIRMA, entre otros. Por lo tanto, se anima a las empresas a que se vayan proveyendo de certificados digitales.
- **La capacidad.** En muchos casos, y en especial en los casos de la empresa, no sólo hace falta garantizar que la persona que se relacio-

na con la Administración es quién dice que es, sino que tiene capacidad para vincular su actuación a la de la empresa: *capacidad de representación*. En este caso, lo que hace falta es:

– Que el certificado digital disponga de atributos en los cuales conste la representación de la persona dentro de la empresa. Para determinados trámites hace falta garantizar esta capacidad.

– Que el certificado digital disponga de atributos en los cuales conste la vinculación de esta persona dentro la empresa.

– En este segundo caso, se podría garantizar la representación o el apoderamiento, no a través del atributo dentro del certificado (en algunos casos esto es difícil de estandarizar), sino acompañando un documento electrónico, firmado digitalmente por un fedatario público donde conste el detalle del apoderamiento y, por lo tanto, dejar en manos de la Administración la validación de estos apoderamientos. Esto empieza a ser posible con los notarios, puesto que todos los notarios de España disponen ya de firma electrónica y están habilitados para generar copias auténticas digitales de escrituras públicas en papel.

– Una alternativa a la opción anterior consistiría en que la empresa autorice a la Administración a consultar esta representación en registros públicos donde conste y que, por lo tanto, no haga falta aportar esta información. Esto, aun cuando puede parecer lo más cómodo, actualmente está disponible en muy pocos casos, dado que depende de que estos registros públicos pongan a disposición de la Administración esta información por medios telemáticos.

– Hay un tercer caso muy específico para relaciones tributarias, que gracias a una disposición especial de la Agencia Tributaria permite poderse relacionar mediante certificados de persona jurídica. Este caso, poco compartido por el resto de administraciones, genera una doble necesidad a la empresa: por una parte, debe dotarse de certificados digitales de atributos para la relación con la mayoría de administraciones y debe dotarse de certificados de persona jurídica para las relaciones tributarias.

En este aspecto animaríamos a las empresas a dotarse de certificados digitales de pertenencia a la empresa y de representación de ésta, como los de CAMERFIRMA y ANCERT entre otros. También recomendaríamos que, en el momento en que se haya de ir al notario, se pidan no sólo co-

pias simples de los documentos, sino también copias simples electrónicas de éstos, firmadas electrónicamente por el notario.

Con respecto a los certificados de persona jurídica, y teniendo en cuenta el bajo coste que tienen, también consideramos importante que cada empresa tenga uno, bajo la custodia del máximo responsable de la empresa, para relaciones tributarias con la Administración.

En algunos casos, algunas administraciones permiten presentar documentos en formato electrónico que han sido generados a partir del escaneo del documento original en papel y firmados por la persona titular del documento. Esta es una iniciativa interesante y muy recomendable para las empresas, dado que permite la compulsa interna de documentos sin necesidad de acudir a un tercero para garantizar su autenticidad. En cualquier caso, será facultad de la Administración admitirla o no y dependerá del trámite en cuestión.

- **La integridad.** Los documentos que se deben presentar a la Administración deben ser íntegros, por lo cual es necesaria la firma electrónica. Las empresas también deben requerir que la información transmitida por parte de la Administración sea íntegra, por lo tanto, es importante empezar a validar la firma electrónica de los documentos recibidos: documentos que han pasado por registros de entrada/salida como prueba de presentación documental ante la Administración, resoluciones que han emitido las administraciones públicas, comprobantes de ingreso, etc.

  Estos documentos se deben conservar en el tiempo. También será bueno empezar a pensar dónde guardarlos y cómo garantizar la validez jurídica del documento.

  Junto a este proceso de comunicación íntegra, también es aconsejable que las empresas empiecen a utilizar plataformas de notificación telemática, como la que las administraciones públicas catalanas están utilizando a través del Consorcio AOC, o la de Correos, para poder recibir comunicaciones con validez jurídica por parte de las administraciones públicas sin necesidad de desplazamientos.

- **El sello de fecha y hora.** Actualmente hay diferentes proveedores que dan servicio de sello de tiempo. Aconsejamos que los documentos incorporen el sello de tiempo en el momento de la firma, dado que esto no sólo da valor legal de autenticidad al documento, sino tam-

bién prueba cuándo fue creado y enviado. Las empresas deberán escoger los proveedores de este servicio.

Finalmente, se anima a todas las empresas a trabajar para poder emitir facturas telemáticas. Próximamente, tal y como ya se ha comentado en el apartado legal, las administraciones públicas sólo aceptarán la factura telemática, por lo cual las empresas deben ir introduciendo esta nueva forma de facturación.

LIBRO BLANCO

GLOSARIO DE TÉRMINOS

Glosario

1_CONCEPTOS

1.1_Término/Definición

ACL Access Control List: listas de control de acceso que permiten controlar los permisos sobre los recursos gestionados: ficheros, bases de datos, aplicaciones, etc.

Adware Software utilizado para la distribución de contenidos publicitarios, cuya introducción en el sistema no ha sido autorizada por el usuario. En muchos casos estas aplicaciones pueden espiar el seguimiento del usuario por la red.

Agujero de seguridad Un agujero de seguridad es un fallo en un programa que permite mediante su explotación violar la seguridad de un sistema informático.

Algoritmos criptográficos Los algoritmos que tienen por finalidad el tratamiento del secreto de la información se llaman criptográficos y son esenciales para la firma electrónica avanzada, ya que soportan el uso de cifras seguras para la producción y comprobación de la firma electrónica.

Un algoritmo es una función matemática ejecutada por un producto informático, formado habitualmente por un hardware y un software.

Análisis forense Se refiere a la recopilación de evidencias que puedan servir como prueba judicial. Es por ello que la mayor parte de las técnicas se basan en la recuperación de información de discos duros.

Antidialers Programas que controlan el marcado automático del teléfono a sitios externos, este ataque es efectivo si tenemos configurado el sistema para acceder a Internet vía línea telefónica común y módem.

Antispam toolkit Caja de herramientas para combatir el spam (mensajes no solicitados).

Antivirus Los antivirus son programas cuya función es detectar y eliminar virus informáticos y otros programas maliciosos (a veces denominados malware).

Applet Una parte pequeña de un programa que se ejecuta con otro programa.

Atributos Es toda información o circunstancia personal que ayuda a identificar de forma unívoca a una persona o a relacionarse con la misma.

Como ejemplos clásicos de atributos podemos citar la representación de otro, los permisos y los privilegios, el domicilio o la dirección electrónica de una persona.

Los atributos pueden contenerse en el certificado o en la firma electrónica. En el primer caso, el prestador que lo emite debe proceder a comprobarlos, de acuerdo con el procedimiento correspondiente, y se podrán emplear siempre de acuerdo con la finalidad específica del certificado.

Autenticación Control (mecanismo técnico o de procedimiento) de seguridad informática que nos permite comprobar la identidad de una entidad (que represente a una persona o a un software informático) que antes habíamos identificado, o que unos datos provienen de un origen conocido (ISO/IEC 10181-2, y también ISO/IEC 7498-2).

B2G Es la abreviatura del término inglés Business to Government y hace referencia a la optimización de los procesos de relación entre las empresas y la Administración pública a través del uso de Internet.

BIAS Aseguramiento de la identidad con biometría.

Biometría La aplicación de técnicas matemáticas y estadísticas sobre los rasgos físicos o de conducta de un individuo.

BOT Diminutivo de Robot. Es un programa diseñado para automatizar tareas. Utilizado de forma maliciosa permite que un intruso controle un ordenador remoto. Los bots se pueden utilizar para mandar spam, descargar y guardar archivos ilegales, atacar a otros ordenadores, robo de información, etc. A los ordenadores infectados por bots se les suele llamar «ordenadores zombis».

Botnet Término que hace referencia a una colección de software robots, que ejecutan de manera autónoma (normalmente un gusano que va por un servidor infectando con capacidad de infectar otros servido-

res). El artífice de la *botnet* puede controlar otros ordenadores/servidores de forma remota y normalmente son poco éticos.

Caballo de Troya, Troyano Programa que aparentemente realiza una función, pero que en realidad realiza otra. No siempre es malicioso o destructivo, pero sus propósitos suelen serlo.

Cardspace Es un software cliente que permite a los usuarios proveer su identidad digital a servicios online de una forma sencilla, segura y en un entorno de confianza.

CATA Servicio de Inteco de alerta rápida antivirus. Tiene como misión principal concienciar en materia de seguridad, ofreciendo alertas, información, herramientas de protección gratuitas e informes diarios de seguridad sobre los últimos códigos maliciosos aparecidos en la Red desde 2001.

CERT Equipo de Seguridad para la Coordinación de Emergencias en Redes Telemáticas, sus funcionas principales son: asesorar, prevenir y resolver incidencias de seguridad en entornos telemáticos.

Certificado de profesional colegiado Certificado digital en el que además de la identidad personal se indica su colegiación en un colegio profesional.

Certificado de representación de órgano administrativo Certificado digital en el que deben tomarse en cuenta los apoderamientos y capacidades de actuación de la persona, indicadas o no en el certificado, antes de confiar en la firma. Debe incluir como subtipos los certificados de representación orgánica, voluntaria, etc.

Certificado de servidor seguro Certificado para dispositivo informático que se instala en un servidor y sirve para cifrar las comunicaciones con este servidor. También sirve para garantizar la identidad del servidor.

Certificado digital Un certificado digital o electrónico es un documento electrónico firmado que garantiza, ante las terceras personas que los reciban o los utilicen, una serie de manifestaciones contenidas en el mismo.

Certificado digital de empleados Certificado digital en el que además de la identidad personal se indica su vinculación con una organización, sin indicación de apoderamiento.

Certificado digital de persona física El certificado de persona física es el que se emite a un usuario individual, que se llama suscriptor del certificado, que será el firmante –en certificados de clave pública de firma– o el que descifre los documentos protegidos con su clave pública –en certificados de cifrado.

Certificado digital de persona jurídica El certificado de persona jurídica –que no existe en la Directiva 99/93/CE– no se define en la Ley 59/2003, pero a partir del artículo 7 de la Ley, que lo regula, podemos describirlo como el que permite imputar la calidad de autor de los documentos directamente a la persona jurídica (apartado 4), siempre que estos documentos se hayan firmado dentro de una relación con las administraciones públicas o dentro del giro o tráfico ordinario de la persona jurídica (apartado 3).

Parece que las aplicaciones del certificado de persona jurídica tengan que ver más con la producción de documentos originales imputables a la entidad que con la firma escrita del apoderado de la entidad.

El certificado de persona jurídica, sin embargo, realmente puede calificarse de certificado de persona física, porque es necesario que lo solicite, en nombre de la persona jurídica, su administrador, representante legal o voluntario con poder suficiente a este efecto (apartado 1), que se llama «custodio».

Certificado ordinario El certificado ordinario es, de acuerdo con el artículo 6 de la Ley 59/2003, de 19 de diciembre, de firma electrónica, «un documento firmado electrónicamente por un prestador de servicios de certificación que vincula unos datos de validación de firma a un firmante y confirma su identidad».

Se llama «ordinario» para diferenciarlo del certificado «reconocido» –una traducción ambigua, por cierto, del término original de la Directiva 99/93/CE, de 13 de diciembre, de firma electrónica, que quizá se debería haber traducido como «certificado cualificado».

Certificado para dispositivos informáticos Certificado digital para identificar servidores seguros, aplicaciones informáticas, firma de código o estampación de fecha y hora.

Certificado reconocido Los certificados reconocidos son, de acuerdo con el artículo 11.1 de la Ley 59/2003, «los certificados electrónicos emi-

tidos por un prestador de servicios de certificación que cumpla los requisitos establecidos en esta Ley en cuanto a la comprobación de la identidad y el resto de circunstancias de los solicitantes, y a la fiabilidad y a las garantías de los servicios de certificación que prestan».

CHAMBER E VAUL Depósito seguro de ficheros de empresa, para los cuales se emite de forma automática un certificado digital de notaría, custodiado por la red mundial de cámaras y despachos de abogados.

CHAMBERTRUST El sello electrónico de las cámaras de comercio.

Cibercriminalidad (cibercrim) Delincuencia informática (criminalidad informática).

Ciberdelitos Cometer un delito informático.

Ciberseguridad Lucha contra la piratería informática.

Cifra Es un mecanismo criptográfico para proteger una información (sea una comunicación en tránsito o un documento más o menos perdurable) de forma que los terceros no autorizados no puedan acceder a ella.

El cifrado se basa en el uso de claves para mezclar o sustituir la posición de los signos alfabéticos y numéricos que componen el documento, operación que se llama «cifrar» (atención al uso del incorrecto término «encriptar»).

La clave aporta la información necesaria para devolver el documento, ahora mezclado y, por lo tanto, ininteligible, a su estado original, operación que se llama «descifrar» (atención al uso del incorrecto término «desencriptar»).

Los cifrados pueden ser simétricos o asimétricos.

Clave criptográfica Las claves criptográficas son los elementos numéricos que forman una cifra criptográfica, y que funcionan conjuntamente con los algoritmos criptográficos para generar firmas electrónicas y las formas de autenticación o para convertir en confidencial un documento.

Clave privada Una clave privada criptográfica es un dato numérico, que forma parte de una cifra, y que debe ser absolutamente secreta, porque sirve para autenticarse, firmar o acceder a datos confidenciales.

Clave pública Una clave pública criptográfica es un dato numérico, que forma parte de una cifra, y que debe ser pública, porque sirve para validar la firma electrónica de un mensaje recibido. El hecho de que sea lo

más pública posible, hace que sea necesario certificar la clave, en asociación con su titular, que posee la clave privada, para que se pueda entregar esta clave pública certificada a través de la red Internet y que llegue a cualquier potencial destinatario de documentos firmados.

Código ejecutable Software que se puede ejecutar en un ordenador.

Confidencialidad Es un estado en el que se puede encontrar una comunicación o un documento electrónico, en el que la comunicación o el documento son secretos para todas las personas, excepto aquellas que, debidamente autorizadas, disponen de los elementos para acceder al contenido de la comunicación o del documento electrónico.

Cookies Fragmento de información que se almacena en el disco duro del visitante de una página web a través de su navegador, a petición del servidor de la página. Esta información puede ser luego recuperada por el servidor en posteriores visitas.

Criptografía Ciencia que trata la protección de la información mediante el desorden por transposición o sustitución (*cryptós*) de las letras (*graphós*) de un documento, con el objetivo de hacerlo confidencial.

La aplicación de la criptografía a las tecnologías de la información y la comunicación se basa en algoritmos y claves correspondientes a las diferentes cifras, simétricas y asimétricas, que se utilizan.

CRL: Lista de revocación Una lista de revocación de certificaciones electrónicas es un mecanismo técnico que tiene como finalidad informar a los terceros destinatarios de mensajes o documentos firmados de los certificados que se encuentran suspendidos o que han sido revocados y que, por lo tanto, no se pueden utilizar para verificar una firma electrónica o, por el contrario, de que la certificación es vigente y la firma puede producir efectos jurídicos.

Cyber Corps Grupo de especialistas de seguridad informática que se encargan de detectar ciberterrorismo.

Dialers Programa que marca un número de teléfono, usando el módem, para la conexión a Internet. Se debe tener precaución con estos programas puesto que a veces llaman a números de tarificación adicional (NTA), estos NTA son números cuyo coste es superior al de una llamada nacional. Estos marcadores se suelen descargar tanto con autorización del usuario (utilizando pop-ups poco claros) como automáticamente.

Direcciones de red IP Es un número que identifica de manera lógica y jerárquica a una interfaz de un dispositivo (habitualmente un ordenador) dentro de una red que utilice el protocolo IP (Internet Protocol).

Dispositivo seguro de creación de firma electrónica Un dispositivo seguro de creación de firma electrónica es un dispositivo que, de acuerdo con el artículo 24.3 de la Ley 59/2003, cumple los siguientes requisitos:

- Los datos utilizados para la generación de la firma electrónica (es decir, la clave privada) pueden producirse sólo una vez y asegura razonablemente su secreto.
- Existe una seguridad razonable de que los datos utilizados para la generación de la firma electrónica no se pueden derivar de los datos de verificación de firma (propiedad de irreversibles) o de la propia firma y de que la firma está protegida contra la falsificación con la tecnología existente en cada momento (longitud de claves).
- Los datos de creación de la firma electrónica pueden ser protegidos de forma fiable por el firmante frente a su utilización por terceros (datos de activación de la creación de firma).
- El dispositivo no altera los datos o el documento que tiene que ser firmado ni impide que éste se muestre al firmante antes del proceso de firma.

El dispositivo seguro es uno de los elementos requeridos para obtener una firma electrónica reconocida, directamente equivalente a la firma escrita, aunque las firmas electrónicas producidas con dispositivos que no gozan de esta consideración también pueden tener efectos, especialmente mediante un pacto entre las partes o una norma administrativa.

DMZ Zona desmilitarizada, también conocida por sus siglas en inglés, DMZ o «de-militarized zone» (DMZ), es un área de la red (una subred) que está situada entre la red interna de una empresa y una red externa, generalmente Internet.

DNI electrónico El Documento Nacional de Identidad electrónico es, de acuerdo con el artículo 15.1 de la Ley 59/2003, de 19 de diciembre, de firma electrónica, el documento nacional de identidad que acredita electrónicamente la identidad personal de su titular y que permite la firma electrónica de documentos.

Corresponde esta definición funcional a un certificado electrónico reconocido de firma electrónica, ultrapasando con mucho la función estricta del documento nacional de identidad del que disponemos en el mundo físico.

DRM Tecnologías de gestión de derechos de autor en el ámbito digital.

DSS Servicios de firma digital.

DUCA Declaración del uso y la contaminación del agua.

EDI Intercambio electrónico de datos (en inglés Electronic Data Interchange o EDI), es un software Middleware que permite la conexión a distintos sistemas empresariales como ERP o CRM. El Intercambio Electrónico de Datos puede realizarse en distintos formatos: EDIFACT (Electronic Data Interchange for Administration, Transport and Commerce), XML, ANSI ASC X12, etc.

Evento o incidencia de seguridad Es un estado identificado en un sistema, servicio o red que indica una posible violación de la política de seguridad, un fallo de los controles de seguridad, o una situación previamente desconocida que pueda tener relevancia para la seguridad.

Factura electrónica La factura electrónica (o efactura) es una modalidad de factura en la que no se emplea el papel como soporte para demostrar su autenticidad. Por eso, la factura electrónica es un fichero que recoge la información relativa a una transacción comercial y sus obligaciones de pago y de liquidación de impuestos y cumple otros requisitos que dependen de la legislación del país en el que se emplea.

FAR Ratio de Falsa Aceptación. Representa el porcentaje de usuarios no autorizados que son correctamente identificados como usuarios válidos.

Firewall El cortafuegos es un elemento utilizado en redes de ordenadores para controlar las comunicaciones, permitiéndolas o prohibiéndolas.

Firma digital La firma digital es una transformación matemática de un documento, realizada mediante una operación de cifrado asimétrico con la clave privada de una persona, frecuentemente llamada firmante.

ISO/IEC 7498-2 define la firma digital como los datos anexados a otros datos, o una transformación criptográfica de éstas, que permite al receptor de estos datos probar el origen de los datos y protegerse de su falsificación posterior.

El hecho de emplear una cifra asimétrica permite que cualquier persona que tenga la clave pública del firmante pueda comprobar que la firma fue generada por la persona que poseía la clave privada, y por lo tanto, que es el autor del documento.

Dado que las cifras criptográficas asimétricas más utilizadas, basadas en multiplicaciones de números primos, incrementan mucho el volumen del documento a firmar, normalmente se resume criptográficamente el documento, antes de producir la firma, que se hará realmente sobre el resumen.

La firma digital es un concepto técnico, referido a una tecnología concreta, y se diferencia del concepto legal de firma, que trata de ser neutral, para dar cobertura a la firma digital, pero también a otras tecnologías que sirvan para las funciones de la firma escrita.

Firma electrónica La firma electrónica es un concepto legal, neutral desde una perspectiva tecnológica, que da cobertura al uso de cualquier tecnología que permita obtener las mismas funciones, con técnicas electrónicas, informáticas y telemáticas, que cumple la firma de documentos en soporte papel.

Estas funciones han sido identificadas, sin voluntad de ser exhaustivo, a la especificación técnica CEN CWA 14365:

- Autenticación de una persona previamente identificada.
- Autenticación del origen de unos datos.
- Declaración de conocimiento.
- Declaración de voluntad.

Todas las tecnologías que permiten cumplir algunas o todas de estas funciones se consideran legalmente como firma, y todas tienen la oportunidad de ser válidas y consideradas como prueba judicial (Ley 59/2003, de 19 de diciembre, de firma electrónica).

Firma electrónica avanzada La firma electrónica avanzada es, de acuerdo con el artículo 3.2 de la Ley 59/2003, la firma electrónica que:

- Identifica al firmante.
- Permite detectar cualquier cambio posterior de los datos firmados.
- Está vinculada al firmante y a los datos firmados de manera única.
- Ha sido creada mediante medios que el firmante puede mantener bajo su control exclusivo.

Definición que se corresponde con la firma digital.

Firma electrónica ordinaria La firma electrónica ordinaria es todo mecanismo tecnológico que nos permita autenticar a la entidad o persona que hace uso de ella.

El artículo 3.1 de la Ley 59/2003 determina, en este sentido, que la firma electrónica ordinaria es el conjunto de datos en forma electrónica, consignados junto a otros o asociadas con ellas, que pueden ser utilizadas como medio de identificación del firmante (donde debemos entender «identificación» como «autenticación de entidades», como correctamente realiza la Directiva 99/93/CE, de 13 de diciembre, de firma electrónica).

Firma electrónica reconocida La firma electrónica reconocida es, en general, todo mecanismo tecnológico que nos permite obtener la autenticidad documental electrónica; es decir, todo mecanismo con el que podamos proteger la integridad de los documentos electrónicos, autenticar al autor de los mismos y le podamos imputar esta calidad de autor.

En concreto, el artículo 3.3 de la Ley 59/2003, de 19 de diciembre, de firma electrónica, considera firma electrónica «la firma electrónica avanzada basada en un certificado reconocido y generado mediante un dispositivo seguro de creación de firma».

Por su lado, el artículo 3.4 determina que la firma electrónica tenga «respecto de los datos consignados en forma electrónica, el mismo valor que la firma electrónica en relación con los consignados en papel».

Esta norma constituye una muestra de la aplicación del principio de equivalencia funcional, y sus consecuencias jurídicas son las siguientes:

- Permite emplear una firma electrónica cuando la normativa requiera una firma escrita.
- Considera el fichero informático firmado como documento electrónico, equivalente al documento escrito a todos los efectos legales.
- Considera la firma electrónica como la firma de la persona, y le imputa el documento, original, en calidad de autor.

La firma electrónica reconocida ofrece el nivel más elevado de garantía de la firma electrónica, y dispone de un procedimiento especial para probar su existencia y corrección técnica.

Fishing Robo de contraseñas mediante links en el correo electrónico que nos trasladan a sitios web fraudulentos pero con un aspecto igual al original. Normalmente en servicios bancarios.

FRR Ratio de Falso Rechazo. Representa el porcentaje de usuarios autorizados que han sido rechazados.

Gestión de identidades Sistema integrado de políticas y procesos organizacionales que pretende facilitar y controlar el acceso a los sistemas de información y a las instalaciones.

El concepto generalmente se relaciona con la informática, medio en el que se ha vuelto cada vez más crítico proteger la información personal, las bases de datos y las aplicaciones tanto personales como profesionales, del uso más o menos malintencionado de los usuarios propios y del espionaje y sabotaje de intrusos. Últimamente también ha devenido su uso con la digitalización de la identidad con la que se controla los accesos físicos de personas, como la entrada y salida de edificios e instalaciones generales o especiales, por medio de tarjetas (electrónicas o magnéticas) y dispositivos biométricos.

Representa una categoría de soluciones interrelacionadas que se utilizan para administrar autenticación de usuarios, derechos y restricciones de acceso, perfiles de cuentas, contraseñas y otros atributos necesarios para la administración de perfiles de usuario en una hipotética aplicación.

Gusanos Los gusanos son un subconjunto de los virus. Tienen la habilidad de reproducirse por sí mismos sin ayuda de personas. Típicamente, los gusanos explotan vulnerabilidades en los servicios de red de los sistemas, por lo que se propagan rápidamente entre sistemas vulnerables. Probablemente, el tipo de gusano más común es el que utiliza el correo electrónico para transportarse. En este caso, el correo electrónico no está infectado, pero transporta el gusano.

Hoax (bulos) Intento de hacer creer a un grupo de personas que algo falso es real. Su objetivo es saturar las redes de comunicaciones, hacer creer a los usuarios que están infectados por algún tipo de virus, saturar el correo electrónico, etc.

Hosting Albergue de los servicios en máquinas propiedad del proveedor.

Housing Albergue de un equipo del cliente en instalaciones del proveedor.

HTTPS El protocolo HTTPS es la versión segura del protocolo HTTP. El sistema HTTPS utiliza un cifrado basado en las Secure Socket Layers (SSL) para crear un canal cifrado (cuyo nivel de cifrado depende del servidor remoto y del navegador utilizado por el cliente) más apropiado para el

tráfico de información sensible que el protocolo HTTP. Cabe mencionar que el uso del protocolo HTTPS no impide que se pueda utilizar HTTP. Es aquí, cuando nuestro navegador nos advertirá sobre la carga de elementos no seguros (HTTP), estando conectados a un entorno seguro (HTTPS).

idCAT Identidad digital catalana.

Identidad digital Sistema de identificación a través de medios electrónicos. El idCAT y el DNI electrónicos son uno de los mecanismos para garantizarla.

IDS (control preventivo) La detección de intrusiones es el proceso de monitorizar los eventos que ocurren en un sistema o red, para analizarlos en busca de problemas de seguridad en base a patrones predefinidos que ofrecen indicios de que el sistema puede estar siendo objeto de un ataque.

Integridad La integridad es una propiedad del documento electrónico que nos informa del hecho que el mismo no ha sido modificado o manipulado de otra forma sin que podamos saberlo (ISO/IEC 7498-2).

En consecuencia, la integridad es uno de los elementos necesarios para disponer de documentos electrónicos auténticos.

El requisito de la integridad es esencial para la firma electrónica que se tenga que equiparar a la firma escrita. Sin el requisito de la integridad, no se puede hablar legalmente de firma electrónica avanzada, ya que el artículo 3.2 de la Ley 59/2003, de firma electrónica, determina que la firma electrónica avanzada debe permitir detectar cualquier cambio posterior de los datos firmados.

Este aspecto es una de las diferencias entre la firma escrita y la firma electrónica, ya que la firma escrita no garantizaba que el documento electrónico no se pudiese manipular (función que cumplía el soporte en papel, mediante la posibilidad de detectar los cambios físicos que este soporte sufría con los rayados y raspados no salvados específicamente por las partes).

Esta propiedad se puede conseguir mediante el uso de algoritmos de resumen, algoritmos de firma o mediante una combinación de ambos algoritmos.

Interoperabilidad (interoperable) Capacidad de comunicación entre diferentes programas y máquinas de diferentes fabricantes.

Irrefutabilidad (no repudio): Autenticidad La autenticidad es una propiedad del documento electrónico que nos informa del hecho que el documento:

- Es íntegro, y por lo tanto, no ha sido modificado sin conocimiento del autor o del destinatario.
- Proviene de una persona identificada y conocida.
- El documento es imputable a la persona, en calidad de autor o en otra calidad concreta, igualmente conocida.

Los ficheros de datos informáticos con esta propiedad cumplen los requisitos legales que se prevén para los documentos (en soporte papel) originales y auténticos.

Esta idea quizá es la más importante que se deriva de la Ley 59/2003: los documentos con firma electrónica son originales (a diferencia de los documentos copia) y son auténticos y, por lo tanto, cuando una ley exige que un acto jurídico debe documentarse, se puede hacer electrónicamente si el documento electrónico tiene la propiedad de la autenticidad.

La autenticidad documental electrónica no cambia la naturaleza del documento, de forma que el documento privado debe ser reconocido por el autor, de acuerdo con el mismo que rige en el mundo presencial. En caso de que el firmante niegue la autenticidad del documento, se practicará la prueba de la firma electrónica y, cuando sea positiva, se declarará que el documento es auténtico.

ISAC Centros de asistencia e intercambio de información de seguridad.

ISO 17799 ISO/IEC 17799 es un estándar para la seguridad de la información publicado por primera vez como ISO/IEC 17799:2000 por International Organization for Standardization y por la comisión International Electrotechnical Commission en el año 2000 y con el título de Information technology - Security techniques - Code of practice for information security management.

Proporciona recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables en iniciar, implantar o mantener sistemas de gestión de la seguridad de la información.

La versión de 2005 del estándar incluye las siguientes once secciones principales:

- Política de seguridad
- Aspectos organizativos para la seguridad
- Clasificación y control de activos
- Seguridad ligada al personal
- Seguridad física y del entorno
- Gestión de comunicaciones y operaciones
- Control de accesos
- Desarrollo y mantenimiento de sistemas
- Gestión de incidentes de seguridad de la información
- Gestión de continuidad de negocio
- Conformidad

IT Tecnologías de la información.

ITIL (The IT Infrastructure Library), un método de organización de los servicios de IT, basado en el concepto de servicios y procesos, en el que la disponibilidad y continuidad del servicio no son procesos ligados a la seguridad, sino a la prestación del servicio.

J2EE Java Platform, Enterprise Edition o Java EE (anteriormente conocido como Java 2 Platform, Enterprise Edition o J2EE hasta la versión 1.4), es una plataforma de programación –parte de la Plataforma Java– para desarrollar y ejecutar software de aplicaciones en lenguaje de programación Java con arquitectura de *n* niveles distribuida, basándose ampliamente en componentes de software modulares ejecutándose sobre un servidor de aplicaciones.

Keylogger Registro de las pulsaciones que se realizan sobre el teclado.

LDAP LDAP (Lightweight Directory Access Protocol) es un protocolo a nivel de aplicación que permite el acceso a un servicio de directorio ordenado y distribuido para buscar diversa información en un entorno de red. LDAP también es considerado una base de datos (aunque su sistema de almacenamiento puede ser diferente) al que pueden realizarse consultas.

Habitualmente, almacena la información de login (usuario y contraseña) y es utilizado para autenticarse aunque es posible almacenar otra información (datos de contacto del usuario, ubicación de diversos recursos de la red, permisos, certificados, etc).

En conclusión, LDAP es un protocolo de acceso unificado a un conjunto de información sobre una red.

Malware Término utilizado para describir de forma genérica cualquier tipo de software o código malicioso.

Medidas correctivas Medidas que se toman una vez producido el incidente.

NAS Network Attached Storage. Es el nombre dado a una tecnología de almacenamiento dedicada a compartir la capacidad de almacenamiento de un servidor con PCs o servidores clientes a través de una red.

OCSP (Online Certificate Status Protocol). Servicio de consulta del estado de los certificados. La consulta se realiza accediendo a un servicio online y recibiendo una respuesta inmediata sobre el estado del certificado en cada momento.

OTP: One Time Password Contraseña dinámica, es decir la contraseña o palabra de paso no puede ser usada más que una vez. Es decir, en el servidor de autenticación existe un algoritmo que genera claves distintas cada cierto período de tiempo, estos generadores están sincronizados con el token de usuario.

PASSI Plataforma de CATCert de atributos de seguridad y firma electrónica.

PDA Personal Digital Assistant (ayudante personal digital) es un ordenador de mano originalmente diseñado como agenda electrónica (calendario, lista de contactos, bloc de notas y recordatorios) con un sistema de reconocimiento de escritura. Actualmente se puede usar como un ordenador doméstico (ver películas, crear documentos, juegos, correo electrónico, navegar por Internet, escuchar música, etc.).

PECAP Plataforma electrónica de contratación de las administraciones públicas.

Phishing Ataque de ingeniería social que tiene como propósito la obtención de información personal sensible del usuario, como contraseñas a la banca electrónica y los códigos de firma, números de tarjetas de crédito. La forma de realizar el ataque es el uso del envío masivo de correos electrónicos en el que el atacante se hace pasar por una persona o empresa de confianza (sobre todo entidad financiera) pidiendo de forma aparentemente

legítima dicha información sensible. El ataque también se puede realizar por medios de mensajería instantánea o incluso por medios telefónicos.

PIN Número personal de identificación.

PKI La infraestructura de claves públicas, también llamada frecuentemente por su denominación inglesa (*Public Key Infrastructure*) y por el acrónimo inglés PKI, es el sistema técnico, jurídico, de seguridad y de organización que ofrece apoyo a los servicios de certificación y de firma electrónica.

Desde la perspectiva de las aplicaciones y de los usuarios de la firma electrónica, este sistema es una infraestructura que debe existir previamente a poder empezar a trabajar con la firma electrónica.

La infraestructura se llama «de claves públicas» porque las operaciones de firma y cifrado requieren como elemento fundamental la publicación y la distribución de las claves públicas de los usuarios de los servicios, en forma de certificados electrónicos de clave pública.

Los integrantes de esta infraestructura pueden ser técnicos o entidades que cumplen un rol o prestan servicios, incluyendo las llamadas autoridades o entidades de certificación, registro, sellos de tiempo y de validación.

Las relaciones que se establecen entre estos sujetos determinan la topología de la infraestructura de clave pública; es decir, la forma y el alcance del sistema de certificación.

Por otro lado, las relaciones internas entre las autoridades de certificación y entre éstas y los usuarios determinan el modelo de confianza de la infraestructura de claves públicas.

Política de seguridad Política que define, a nivel estratégico, las principales directrices y líneas de actuación en seguridad de forma muy general, estableciendo así los principios, objetivos y responsabilidades y marco de actuación por la Dirección de la Organización.

Políticas de contraseñas Una política de contraseña es un conjunto de normas de seguridad, técnicas, de organización, legales y de negocio referidas a un servicio de contraseñas, consistente en generar, verificar y gestionar posteriormente a los usuarios y sus contraseñas.

Programa espía Ver Spyware.

Programa malicioso Ver Malware.

PSIS Plataforma de CATCert de servicios de identidad y firma electrónica.

Redes Grid Sistema de computación distribuido que permite compartir recursos no centrados geográficamente para resolver problemas de gran escala. Los recursos compartidos pueden ser ordenadores (PCs, estaciones de trabajo, supercomputadoras, PDA, portátiles, móviles, etc.), software, datos e información, instrumentos especiales (radio, telescopios, etc.), personas/colaboradores…

RELI Registro Electrónico de Empresas Licitadoras.

Rootkit Herramientas diseñadas para controlar de forma oculta, sin que el usuario pueda detectarlo, un ordenador. La utilización de rootkits no debería ser necesariamente maliciosa, ya que son herramientas útiles para la administración remota de los sistemas.

SAML Security Assertion Markup Language (SAML) es un estándar XML para intercambiar información sobre autenticación y autorización entre dominios de seguridad, es decir, entre proveedores de identidades digitales (productores de aserciones) y proveedores de servicios (consumidores de aserciones). SAML es un producto del OASIS Security Services Technical Committee.

Sello de fecha y hora El sellado de tiempo consiste en asociar un documento o transacción a una fecha y hora concreta recogida de una fuente fiable y firmarlo electrónicamente por el prestador del servicio. Un sello de tiempo es una evidencia electrónica de que un documento o transacción existía en una fecha concreta.

Servicio de aprovisionamiento Servicio para gestionar el aprovisionamiento y la asignación de información de identidad y de recursos del sistema dentro de organizaciones y entre éstas.

Single sign on Procedimiento de autenticación que habilita al usuario para acceder a varios sistemas con una sola instancia de identificación.

SLA Service Level Agreement. Es un protocolo plasmado normalmente en un documento de carácter legal por el que una compañía que presta un servicio a otra se compromete a prestar el mismo bajo unas determinadas condiciones y con unas prestaciones mínimas.

El nivel de servicio se basa en indicadores que permiten cuantificar de manera objetiva determinados aspectos del servicio prestado. Por ejemplo un indicador de nivel de servicio puede ser el tiempo de resolución de

incidencias. Este indicador se mide a través de aplicaciones de gestión de incidencias que registran el momento que una incidencia es comunicada y cuándo es cerrada. La diferencia entre estos dos datos es el indicador en bruto desagregado que luego puede ser procesado mediante algoritmos para obtener promedios, desviaciones y otros indicadores normalizados.

SMTP Simple Mail Transfer Protocol (SMTP), o protocolo simple de transferencia de correo electrónico. Protocolo de red basado en texto utilizado para el intercambio de mensajes de correo electrónico entre computadoras o distintos dispositivos (PDA, teléfonos móviles, etc.). Está definido en el RFC 2821 y es un estándar oficial de Internet.

SOAP SIMPLE OBJECT ACCESS PROTOCOL. Es un protocolo estándar creado por Microsoft, IBM y otros, que está actualmente bajo el auspicio de la W3C el cual define cómo dos objetos en diferentes procesos pueden comunicarse por medio de intercambio de datos XML. SOAP es uno de los protocolos utilizados en los servicios web.

SPAM Correo electrónico no deseado, «correo basura».

Spyware (programas espía) Programas que recopilan información sobre una persona u organización sin su conocimiento. Esta información se envía a un punto de recolección y control. El spyware se distribuye tanto como parte de otro programa (como un caballo de Troya), como a través de un gusano o de páginas web que explotan vulnerabilidades de los navegadores.

SSDLC (Secure Software Development Life Cycle). Es el principal marco de referencia en el ámbito del desarrollo seguro de aplicaciones y servicios.

SSL/TSL Protocolo que proporciona autenticación y privacidad de la información entre extremos sobre Internet mediante el uso de criptografía. Normalmente accedemos a este protocolo cuando tecleamos en un navegador https:// en vez del clásico http://.

Taxonomía Tratamiento de las herramientas matemáticas que comporta el estudio de las clasificaciones.

TDT Televisión digital terrestre.

TIC Tecnologías de la información y de las comunicaciones.

Token Objeto físico único para un usuario o un grupo de usuarios que almacena la información necesaria para realizar el proceso de autenticación mediante un protocolo determinado.

Un incidente de seguridad Es uno o varios eventos inesperados de seguridad que tienen una alta probabilidad de comprometer la operativa del negocio y que amenaza la seguridad de la información.

Validación La validación o verificación de los certificados electrónicos o de la firma electrónica de un documento es el procedimiento mediante el cual el tercer destinatario de un documento firmado, que debe comprobar la firma electrónica, puede comprobar la existencia y validez de la certificación del firmante (y de los prestadores de servicios de certificación que emitieron la certificación).

Hay que ejecutar tantas veces el procedimiento de verificación de los certificados individuales como certificados forman parte de una ruta de certificación, con excepción del certificado de la entidad de certificación raíz.

Si todos los certificados de la ruta son válidos y autorizan el uso de las claves para la finalidad concreta que nos interesa, entonces podemos proceder a la validación de la firma electrónica.

Virus Programa que se reproduce a sí mismo de forma exacta o con modificaciones (mutaciones), en otra pieza de código ejecutable. Los virus pueden utilizar diversos tipos de anfitriones: ficheros ejecutables, sectores de arranque, ficheros de scripts y macros de documentos.

WiFi Es un conjunto de estándares para redes inalámbricas basados en las especificaciones IEEE 802.11. Creado para ser utilizado en redes locales inalámbricas, es frecuente que en la actualidad también se utilice para acceder a Internet.

WSS SEGURIDAD SERVICIOS WEB. Protocolo de comunicaciones que suministra un medio para aplicar seguridad a los servicios web. En abril de 2004 el estándar WS-Security 1.0 fue publicado por Oasis-Open.

WS-SX Intercambio seguro de servicios web.

XACML Lenguaje extensible de marcas de control de acceso: Trabaja en la representación y la evaluación de políticas de control de acceso.

XML eXtensible Markup Language. Es un metalenguaje extensible de etiquetas desarrollado por el World Wide Web Consortium (W3C).

XML Dsig XML Digital Signature. También llamada: XML-DSig, XML-Sig es una recomendación del W3C que define una sintaxis XML para la firma digital de documentos.

2_ORGANISMOS

2.1_Términos/Definiciones

ACA Agencia Catalana del Agua

ANCERT Agencia Notarial de Certificación

ASIMELEC Asociación Multisectorial de Empresas Españolas de Electrónica y Comunicaciones

Camerfirma Autoridad de certificación digital de las cámaras de comercio españolas

CATA Centro de Alerta Temprana de Antivirus

CATCert Agencia Catalana de Certificación

CCN Centro Criptológico Nacional

CCN-CERT Equipo de respuesta a incidentes de seguridad de la información

CEI Comisión Electrotécnica Internacional

CEN Comité Europeo de Normalización

CENELEC Comité Europeo de Normalización Electrónica

CIWIN Comisión de la Red de Información sobre Alertas en Infraestructuras Críticas

CN Centro Nacional de Inteligencia

CoE Consejo de Europa

EESSI Iniciativa europea de normalización de firma electrónica

ENAC Entidad de acreditación

ENISA Agencia Europea de Seguridad de Redes y de la Información

ETSI Instituto europeo de normas de telecomunicaciones

ICC Cámara de Comercio Internacional

ICTSB Grupo directivo de seguridad de las redes y la información

IEFT Internet engineering task force: fuerza de trabajo de ingenieros de Internet

INTA Instituto Nacional de Técnica Aeroespacial

INTECO Instituto Nacional de Tecnología de la Comunicación

ISO Organización Internacional de Estandarización

ISSS Information Society Standaritzation System

ITU-T Unión Internacional de Telecomunicaciones, sección de Telecomunicaciones

Liberty Alliance Consorcio formado en 2001 por unas 30 organizaciones para establecer estándares abiertos, líneas de trabajo y casos de éxito en procesos de federación de identidades digitales

NISSG Grupo directivo de redes y de la información

OASIS Organization for the Advancement of Structured Information Standards

OCDE Organización para la Cooperación y el Desarrollo Económico

PEPIC Programa Europeo de Protección de Infraestructuras Críticas

PKIA Adopción de infraestructura de clave pública

Red.es Entidad pública empresarial adscrita al Ministerio de Industria, Turismo y Comercio

RedIRIS Red nacional de investigación y desarrollo

SAAG South Asia Analysis Group

W3C Consorcio World Wide Web

Libro blanco. La seguridad de los negocios en Internet
Noviembre de 2007

Cámara Oficial de Comercio, Industria y Navegación de Barcelona

Director del Libro blanco
Josep Morell, comisionado para la Sociedad de la Información de la Presidencia de la Cámara de Comercio de Barcelona

Coordinadores
Jordi Masías*, *director de CATCert*
Josep Maria Canals, asesor de la Cámara de Comercio de Barcelona

Autores
Ignacio Alamillo, *director de Asesoramiento e Investigación de la Agencia Catalana de Certificación*

Fernando de la Cuadra, *Panda Security*

Jordi Masías*, *director de CATCert*

Ramiro Muñoz, *director técnico de Camerfirma,* CISA

Rafael Ortega, *Socio de Ernst & Young*

Josep Maria Clopés, *director de Negocio de Gematic*

Emma Suevos, *directora de Calidad y Procedimentos de la Agencia Catalana de Certificación*

Cambra de Comerç de Barcelona

CATCert
Agència Catalana de Certificació

La elaboración y edición del ***Libro blanco. La seguridad de los negocios e Internet*** es fruto de la colaboración entre la Cámara Oficial de Comercio, Industria y Navegación de Barcelona y la Agencia Catalana de Certificación

El capítulo «Lista de control, un camino hacia adelante», forma parte de la doctrina compartida con la Cámara de Comercio Internacional, y se incluye disponiendo de los permisos correspondientes

* Director de CATCert hasta el 30 de septiembre, a partir de esta fecha es socio-director de Asesoramiento y Gestión TIC (AGTIC).

Libro blanco. La seguridad de los negocios en Internet
Noviembre de 2007

Cámara Oficial de Comercio, Industria y Navegación de Barcelona

Director del Libro blanco
Josep Morell, comisionado para la Sociedad de la Información de la Presidencia de la Cámara de Comercio de Barcelona

Coordinadores
Jordi Masías*, *director de CATCert*
Josep Maria Canals, asesor de la Cámara de Comercio de Barcelona

Autores
Ignacio Alamillo, *director de Asesoramiento e Investigación de la Agencia Catalana de Certificación*

Fernando de la Cuadra, *Panda Security*

Jordi Masías*, *director de CATCert*

Ramiro Muñoz, *director técnico de Camerfirma,* CISA

Rafael Ortega, *Socio de Ernst & Young*

Josep Maria Clopés, *director de Negocio de Gematic*

Emma Suevos, *directora de Calidad y Procedimentos de la Agencia Catalana de Certificación*

Cambra de Comerç de Barcelona

CATCert
Agència Catalana de Certificació

La elaboración y edición del ***Libro blanco. La seguridad de los negocios e Internet*** es fruto de la colaboración entre la Cámara Oficial de Comercio, Industria y Navegación de Barcelona y la Agencia Catalana de Certificación

El capítulo «Lista de control, un camino hacia adelante», forma parte de la doctrina compartida con la Cámara de Comercio Internacional, y se incluye disponiendo de los permisos correspondientes

* Director de CATCert hasta el 30 de septiembre, a partir de esta fecha es socio-director de Asesoramiento y Gestión TIC (AGTIC).

2. Con efectos para los períodos impositivos que se inicien a partir de 1 de enero de 2007, se da nueva redacción al apartado 4 y se añade un apartado 5 a la disposición adicional décima del texto refundido de la Ley del Impuesto sobre Sociedades, aprobado por Real Decreto Legislativo 4/2004, de 5 de marzo, que quedarán redactados de la siguiente manera:

«4. Las deducciones reguladas en los apartados 1 y 3 del artículo 38 de esta Ley se determinarán multiplicando los porcentajes de deducción fijados en dichos apartados por los coeficientes establecidos en la disposición adicional novena de esta Ley. El porcentaje de deducción que resulte se redondeará en la unidad superior.

5. El porcentaje de deducción establecido en el apartado 2 del artículo 38 de esta Ley será del 18 por ciento. Dicho porcentaje será del 5 por ciento para el coproductor financiero.»

3. Con efectos para los períodos impositivos que se inicien a partir de 1 de enero de 2007, se da nueva redacción a los apartados 2 y 3 de la disposición transitoria vigésima primera del texto refundido de la Ley del Impuesto sobre Sociedades, aprobado por Real Decreto Legislativo 4/2004, de 5 de marzo, que quedarán redactados de la siguiente manera:

«2. Las deducciones establecidas en el artículo 35 y en el apartado 2 del artículo 38 de esta Ley, pendientes de aplicación al comienzo del primer período impositivo que se inicie a partir de 1 de enero de 2012, podrán aplicarse en el plazo y con los requisitos establecidos en el capítulo IV del título VI de esta Ley, según redacción vigente a 31 de diciembre de 2011. Dichos requisitos son igualmente aplicables para consolidar las deducciones practicadas en períodos impositivos iniciados antes de aquella fecha.

3. Las deducciones establecidas en los apartados 1 y 3 del artículo 38 de esta Ley, pendientes de aplicación al comienzo del primer período impositivo que se inicie a partir de 1 de enero de 2014, podrán aplicarse en el plazo y con los requisitos establecidos en el capítulo IV del título VI de esta Ley, según redacción vigente a 31 de diciembre de 2013. Dichos requisitos son igualmente aplicables para consolidar las deducciones practicadas en períodos impositivos iniciados antes de aquella fecha.»

Disposición final tercera. *Títulos competenciales.*

La Ley se dicta al amparo de lo establecido en el artículo 149.2 de la Constitución, que dispone que, sin perjuicio de las competencias que podrán asumir las Comunidades Autónomas, el Estado considerará el servicio de la cultura como deber y atribución esencial, con la excepción de los siguientes artículos:

1. Los artículos 8 y 9 se dictan al amparo del artículo 149.1.1.ª de la Constitución, que reserva al Estado la regulación de las condiciones básicas que garanticen la igualdad de todos los españoles en el ejercicio de los derechos y en el cumplimiento de los deberes constitucionales.

2. Los artículos 7; 10 a 18; 22 y 23; 24 a 27; 28; 31, 32, 33, 34 y 38 a 40, así como la disposición adicional undécima se dictan al amparo del artículo 149.1.13.ª de la Constitución, que reserva al Estado la competencia sobre bases y coordinación de la planificación general de la actividad económica.

3. El artículo 35 se dicta al amparo de lo previsto en el artículo 149.1.15.ª relativo al fomento y coordinación general de la investigación científica y técnica.

4. La disposición adicional séptima se dicta al amparo del artículo 149.1.30.ª de la Constitución relativo a las normas básicas para el desarrollo del artículo 27 de la misma.

5. Las disposiciones adicionales octava y novena se dictan al amparo del artículo 149.1.7.ª de la Constitución, que reserva al Estado la legislación laboral, sin perjuicio de su ejecución por los órganos de las Comunidades Autónomas.

6. La disposición final primera se dicta al amparo del artículo 149.1.6.ª de la Constitución, que reserva al Estado la legislación mercantil.

7. El artículo 21 y las disposiciones adicional cuarta y final segunda se dictan al amparo del artículo 149.1.14.ª que reserva al Estado la competencia sobre la Hacienda General y Deuda del Estado.

Disposición final cuarta. *Desarrollo y habilitación normativa.*

1. Se autoriza al Gobierno a dictar cuantas disposiciones resulten necesarias para la aplicación y desarrollo de la presente Ley en el ámbito de sus competencias.

2. Cuando razones técnicas o de oportunidad así lo aconsejen, el Gobierno, oídas las Comunidades Autónomas, podrá modificar los porcentajes establecidos en el artículo 18 para el cumplimiento de la cuota de pantalla y en el artículo 24 para la minoración de importes de las ayudas a la producción.

Disposición final quinta. *Entrada en vigor.*

La presente Ley entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado» salvo lo dispuesto en el artículo 36, que entrará en vigor el 1 de enero de 2009.

Por tanto,
Mando a todos los españoles, particulares y autoridades, que guarden y hagan guardar esta ley.

Madrid, 28 de diciembre de 2007.

JUAN CARLOS R.

El Presidente del Gobierno,
JOSÉ LUIS RODRÍGUEZ ZAPATERO

22440 *LEY 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información.*

JUAN CARLOS I
REY DE ESPAÑA

A todos los que la presente vieren y entendieren.
Sabed: Que las Cortes Generales han aprobado y Yo vengo en sancionar la siguiente Ley.

PREÁMBULO

I

La presente Ley se enmarca en el conjunto de medidas que constituyen el Plan 2006-2010 para el desarrollo de la Sociedad de la Información y de convergencia con Europa y entre Comunidades Autónomas y Ciudades Autónomas, Plan Avanza, aprobado por el Gobierno en noviembre de 2005.

El Plan Avanza prevé entre sus medidas la adopción de una serie de iniciativas normativas dirigidas a eliminar las barreras existentes a la expansión y uso de las tecno-

logías de la información y de las comunicaciones y para garantizar los derechos de los ciudadanos en la nueva sociedad de la información.

En esta línea, la presente Ley, por una parte, introduce una serie de innovaciones normativas en materia de facturación electrónica y de refuerzo de los derechos de los usuarios y, por otra parte, acomete las modificaciones necesarias en el ordenamiento jurídico para promover el impulso de la sociedad de la información.

En este sentido, se introducen una serie de modificaciones tanto de la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico, como de la Ley 59/2003, de 19 de diciembre, de firma electrónica, que constituyen dos piezas angulares del marco jurídico en el que se desenvuelve el desarrollo de la sociedad de la información.

Dicha revisión del ordenamiento jurídico se completa con otras modificaciones menores de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, de la Ley 11/1998, de 24 de abril, General de Telecomunicaciones y de la Ley 7/1996, de 15 de enero, de ordenación del comercio minorista.

II

El capítulo I de la Ley introduce sendos preceptos dirigidos a impulsar el empleo de la factura electrónica y del uso de medios electrónicos en todas las fases de los procesos de contratación y a garantizar una interlocución electrónica de los usuarios y consumidores con las empresas que presten determinados servicios de especial relevancia económica.

En materia de facturación electrónica, el artículo 1 establece la obligatoriedad del uso de la factura electrónica en el marco de la contratación con el sector público estatal en los términos que se precisen en la Ley reguladora de contratos del sector público, define el concepto legal de factura electrónica y, asimismo, prevé actuaciones de complemento y profundización del uso de medios electrónicos en los procesos de contratación.

Así, el citado precepto prevé que el Gobierno determinará el órgano competente de la Administración General del Estado que impulsará el empleo de la factura electrónica entre los diversos agentes del mercado, en particular entre las pequeñas y medianas empresas y en las denominadas microempresas, de acuerdo con la definición establecida en la Recomendación C(2003) 1422 de la Comisión Europea, de 6 de mayo de 2003, con el fin de fomentar el desarrollo del comercio electrónico. Por su parte, las Comunidades Autónomas, de acuerdo con las competencias que tenga reconocidas por sus Estatutos, colaborarán en coordinación con la Administración del Estado en el empleo de la factura electrónica.

De igual modo el Gobierno, o en su caso las Comunidades Autónomas en el ámbito de sus competencias desarrollarán, en cooperación con las asociaciones representativas de las empresas proveedoras de soluciones técnicas de facturación electrónica y de las asociaciones relevantes de usuarios, un plan para la generalización del uso de la factura electrónica en España, definiendo, asimismo, los contenidos básicos de dicho plan.

Asimismo, la Ley habilita a los Ministerios de Industria, Turismo y Comercio y de Economía y Hacienda, respetando las competencias reconocidas a las Comunidades Autónomas, para que aprueben las normas sobre formatos estructurados estándar de facturas electrónicas que sean necesarias para facilitar la interoperabilidad tanto en el sector público como en el sector privado y permitan facilitar y potenciar el tratamiento automatizado de las mismas.

Además, el citado precepto, yendo más allá del impulso a la extensión del uso de la factura electrónica, encomienda a las diversas Administraciones Públicas en el ámbito de sus competencias la promoción de la extensión y generalización del uso de medios electrónicos en las demás fases de los procesos de contratación.

El artículo 2, por su parte, establece la obligación de las empresas de determinados sectores con especial incidencia en la actividad económica (entre otras, compañías dedicadas al suministro de electricidad, agua y gas, telecomunicaciones, entidades financieras, aseguradoras, grandes superficies, transportes, agencias de viaje) de facilitar un medio de interlocución telemática a los usuarios de sus servicios que cuenten con certificados reconocidos de firma electrónica.

Esta nueva obligación tiene por finalidad asegurar que los ciudadanos cuenten con un canal de comunicación electrónica con las empresas cuyos servicios tienen una mayor trascendencia en el desarrollo cotidiano de sus vidas.

A tales efectos, se especifica que dicha interlocución telemática ha de facilitar al menos la realización de trámites tales como la contratación electrónica, modificación de condiciones contractuales, altas, bajas, quejas, histórico de facturación, sustitución de informaciones y datos en general, así como el ejercicio de sus derechos de acceso, rectificación, oposición y cancelación en materia de protección de datos. Asimismo, se prevé que dicho medio de interlocución telemática sirva para sustituir los trámites que actualmente se realicen por fax. No obstante, el citado precepto no impide que excepcionalmente las empresas obligadas por el mismo no faciliten la contratación de productos o servicios que por su naturaleza no sean susceptibles de comercialización por vía electrónica.

Esta obligación vendrá a complementar la garantía del derecho de una comunicación electrónica de los ciudadanos con las Administraciones Públicas, establecida en la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, en ejecución de uno de los mandatos normativos contenidos en el Plan Avanza.

Por último, el artículo 3 tiene por finalidad establecer una regulación mínima de las subastas electrónicas entre empresarios (B2B) a fin de establecer un marco jurídico que dote a esta técnica de compra de la necesaria transparencia y seguridad jurídica.

En este sentido, la regulación prevista tiene por objeto evitar las suspicacias de las empresas a la hora de participar en estos nuevos métodos de compra y eliminar cualquier tipo de práctica o competencia desleal. En definitiva, se trata de garantizar a través de un precepto específico los principios de igualdad de trato, de no discriminación y transparencia entre empresas.

III

El capítulo II de la Ley engloba las modificaciones legislativas que se han estimado necesarias para promover el impulso de la sociedad de la información y de las comunicaciones electrónicas.

Dichas modificaciones afectan principalmente a la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico y a la Ley 59/2003, de 19 de diciembre, de firma electrónica, si bien se incluyen también modificaciones de menor entidad de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, se modifica la Ley 7/1996, de 15 de enero, de ordenación del comercio minorista para incluir un nuevo tipo de infracción que respalde lo dispuesto en el artículo 2 de la presente Ley, se introducen una serie de cambios en la Ley 11/1998, de 24 de abril, General de Telecomunicaciones y se introducen, asimismo, modificaciones en la Ley de Propiedad Intelectual.

El artículo 4 de la Ley incluye las diferentes modificaciones necesarias en el vigente texto de la Ley 34/2002,

de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI).

Estas modificaciones tienen como finalidad, en primer lugar, revisar o eliminar obligaciones excesivas o innecesarias y, en segundo lugar, flexibilizar las obligaciones referidas a las comunicaciones comerciales y a la contratación electrónicas a fin de, entre otras razones, adecuar su aplicación al uso de dispositivos móviles.

La primera medida prevista es la nueva redacción del artículo 8 que regula las restricciones a la prestación de servicios de la sociedad de la información y su procedimiento de cooperación intracomunitario. Por lo que al primer aspecto se refiere, es decir, las restricciones a los servicios de telecomunicaciones, este precepto establece que en el caso de que un determinado servicio de esta naturaleza atente contra los principios que en el propio precepto se recogen, los órganos competentes para su protección adoptarán las medidas necesarias para que se pueda interrumpir su prestación o retirar los datos que los vulneran. Los principios objeto de protección son: la salvaguarda del orden público, la investigación penal, la seguridad pública y la defensa nacional; la protección de la salud pública o de las personas físicas o jurídicas que tengan la condición de consumidores y usuarios; el respeto a la dignidad de la persona y al principio a la no discriminación por motivos de raza, sexo, religión, opinión, nacionalidad, discapacidad o cualquier otra circunstancia personal o social, y finalmente, la protección de la juventud y de la infancia. Como no puede ser de otra manera, se prevé que en la adopción de estas medidas se respetarán siempre las garantías y procedimientos establecidos en las leyes. Finalmente, sobre este punto de las restricciones a la prestación de servicios de la Sociedad de la Información, el artículo 8 incorpora además el principio de que solo la autoridad judicial competente, en los casos en que la Constitución y las leyes de los respectivos derechos y libertades fundamentales así lo prevean de forma excluyente, podrán adoptar las medidas restrictivas previstas en este artículo, en tanto que garante de los derechos a la libertad de expresión, de producción y creación literaria científica y técnica, de información y de cátedra.

En relación con el procedimiento de cooperación intracomunitario, el vigente apartado 4 del artículo 8 mantiene prácticamente su redacción pues constituye una transposición necesaria del procedimiento intracomunitario de cooperación previsto en la Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior. Por su parte, el vigente apartado 2 del artículo 8, sobre colaboración de prestadores de servicios de intermediación para impedir el acceso desde España a servicios o contenidos cuya interrupción o retirada haya decidido un órgano competente, se traslada al artículo 11.

En coherencia con la nueva redacción del artículo 8 se elimina también el párrafo a) del apartado 2 del artículo 38, por el que se tipifica como infracción administrativa muy grave el incumplimiento de las órdenes dictadas por órganos administrativos en virtud del artículo 8. A este respecto, se considera que los órganos competentes para imponer restricciones en el mundo físico, ya sean judiciales o administrativos –piénsese por ejemplo en las autoridades de control sanitario–, deberán estar habilitados por sus propias normas a imponer dichas restricciones a los prestadores de servicios de la sociedad de la información cuando incumplan una orden emanada por los mismos en ejercicio de sus competencias legalmente atribuidas. Sin perjuicio de lo anterior, la nueva redacción del apartado 4 del artículo 8 remite al artículo 11 para habilitar al órgano competente a requerir la colaboración de los prestadores de servicios de intermediación en caso de estimarlo necesario para garantizar la eficacia de las medidas que hubiera adoptado.

Como consecuencia de las modificaciones realizadas en el artículo 8 se procede a hacer un ajuste técnico en la remisión contenida en el artículo 4 que ahora debe remitirse al artículo 11.

La segunda modificación importante prevista en relación con la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI) es la supresión de la obligación establecida en el artículo 9 sobre constancia registral de los nombres de dominio, dado que se ha revelado como poco operativa desde un punto de vista práctico.

En coherencia con la supresión del artículo 9 se prevé también la eliminación del párrafo a) del apartado 4 del artículo 38 en el que se tipifica como infracción administrativa leve el incumplimiento de lo dispuesto en el artículo 9.

Como consecuencia de la supresión del artículo 9 se procede a una modificación técnica en la redacción del párrafo b) del apartado 1 del artículo 10. Asimismo, se realiza un ajuste de redacción en el párrafo f) del apartado 1 del artículo 10.

En tercer lugar, se ha entendido necesaria la modificación del artículo 11. La redacción vigente del artículo incluye una posibilidad de intervención del Ministerio de Ciencia y Tecnología (hoy Ministerio de Industria, Turismo y Comercio) que se ha eliminado. En este sentido, son los propios órganos competentes los que en ejercicio de las competencias que legalmente tengan atribuidas deben dirigirse directamente a los prestadores de servicios de intermediación, sin que sea necesario que un departamento ajeno, como es el Ministerio de Industria, Turismo y Comercio, intervenga en un procedimiento en el que se diluciden asuntos en los que carece de competencias.

Por otra parte, se precisa en el artículo 11 que la suspensión del servicio que se puede ordenar a los prestadores de servicios de intermediación se circunscribe a aquéllos empleados por terceros para proveer el servicio de la sociedad de la información o facilitar el contenido cuya interrupción o retirada haya sido ordenada. Se añade, además, un nuevo apartado 2, que traslada a este artículo la previsión actualmente establecida en el apartado 2 del artículo 8, que prevé la posibilidad de requerir la colaboración de los prestadores de servicios de intermediación para impedir el acceso desde España a servicios o contenidos cuya interrupción o retirada haya sido decidida.

Igualmente se incluye un nuevo inciso en el apartado 3 del artículo 11 que aclara que la autorización del secuestro de páginas de Internet o de su restricción cuando ésta afecte a los derechos y libertades de expresión e información y demás amparados en los términos establecidos en el artículo 20 de la Constitución solo podrá ser decidida por los órganos jurisdiccionales competentes.

Por otra parte, se incluye un nuevo artículo 12 bis que establece la obligación de los proveedores de acceso a Internet establecidos en España a informar a sus usuarios sobre los medios técnicos que permitan, entre otros, la protección frente a virus informáticos y programas espía, la restricción de los correos electrónicos no solicitados, y la restricción o selección del acceso a determinados contenidos y servicios no deseados o nocivos para la juventud y la infancia.

Igualmente, se obliga a dichos prestadores, así como a los prestadores de servicios de correo electrónico a informar a sus clientes sobre las medidas de seguridad que aplican en la provisión de sus servicios.

Asimismo, se encomienda a los proveedores de servicios de acceso la función de informar a sus clientes sobre las posibles responsabilidades en que puedan incurrir por el uso de Internet con fines ilícitos, en particular, para la comisión de ilícitos penales y por la vulneración de la legislación en materia de propiedad intelectual e industrial. A

fin de respaldar estas obligaciones se incluye un nuevo tipo de infracción leve en el apartado 4 del artículo 38, que, teniendo en cuenta la supresión del vigente párrafo a), dará nuevo contenido al mismo.

Otra modificación considerada necesaria es la revisión de la vigente redacción del apartado 2 del artículo 17 a fin de aclarar y precisar que en virtud del mismo se responsabiliza al proveedor del link o del motor de búsqueda de los contenidos de los que tiene conocimiento cuando hayan sido elaborados bajo su «dirección, autoridad o control».

Se incorpora una nueva redacción al apartado 3 del artículo 18, en el sentido de que los códigos de conducta a que se refiere este precepto deberán ser accesibles por vía electrónica, fomentándose su traducción en las distintas lenguas oficiales del Estado y de la Unión Europea con el fin de proporcionarles la mayor difusión posible.

En materia de comunicaciones comerciales se flexibiliza la exigencia de información prevista en el vigente artículo 20 sobre mensajes publicitarios a través de correo electrónico o medios de comunicación equivalentes de modo que en vez de la inserción del término «publicidad» al inicio del mensaje pueda incluirse la abreviatura «publi». Se trata de una medida que ha sido solicitada en diversas ocasiones por agentes que desarrollan actividades relacionadas con la publicidad a través de telefonía móvil y, por otra parte, no supone menoscabo de la protección y de los derechos de información de los usuarios, ya que el término «publi» es fácilmente reconocible como indicativo de «publicidad».

Adicionalmente, se realizan ajustes menores en la redacción del mencionado artículo a fin de alinearlo en mayor medida con lo dispuesto en la Directiva 2000/31/CE.

En materia de contratación electrónica se realiza un ajuste de la redacción actual del artículo 24 a fin de incluir una remisión expresa a la Ley 59/2003, de 19 de diciembre, de firma electrónica y destacar así el especial valor probatorio de los contratos electrónicos que sean celebrados mediante el uso de instrumentos de firma electrónica.

De igual modo, se ajusta el artículo 27, relativo a las obligaciones de información previa en materia de contratación electrónica, a la luz de la experiencia acumulada en su aplicación por parte del Ministerio de Industria, Turismo y Comercio en ejercicio de sus competencias de inspección y control de páginas de Internet. En este sentido, se prevé que la información que debe facilitarse ha de «ponerse a disposición» de los usuarios «mediante técnicas adecuadas al medio de comunicación utilizado», flexibilizando de este modo la redacción anterior con vistas a facilitar la realización de operaciones de contratación electrónica mediante dispositivos que cuenten con pantallas de visualización de formato reducido.

Asimismo, se incluye en la nueva redacción del artículo 27 una regla aclaratoria por la cual, cuando el prestador de servicios diseñe específicamente sus servicios de contratación electrónica para ser accedidos mediante dispositivos que cuenten con pantallas de formato reducido, se entenderán cumplidas las obligaciones de información previa establecidas en dicho precepto cuando el citado prestador facilite de manera permanente, fácil, directa y exacta la dirección de Internet en que dicha información es puesta a disposición del destinatario.

También se modifica el apartado 2 del artículo 27 a fin de eliminar el inciso «cuando no se utilicen estos medios con el exclusivo propósito de eludir el cumplimiento de dicha obligación» dado que en la práctica es imposible determinar cuando se hace con este propósito.

Este artículo 4 modifica también los artículos 33, 35 y 43 de la Ley 34/2002, de 11 de julio, de Servicios de Sociedad de la Información y del Comercio Electrónico.

Las modificaciones que se introducen a los artículos 33 y 35 tienen por objeto adaptar su contenido a la vigente organización de la Administración territorial del Estado en función de las competencias que tienen atribuidas tanto la Administración General del Estado como aquellas de las Comunidades Autónomas.

Por otra parte, se da una nueva redacción al artículo 43 de la Ley 34/2002 que se refiere a la potestad sancionadora. En concreto, la nueva redacción establece que la imposición de sanciones por incumplimiento de lo establecido en dicha ley corresponderá al órgano o autoridad que dictó la resolución incumplida o al que estén adscritos los inspectores. En el ámbito de las Comunidades Autónomas, las infracciones contra derechos y garantías de los consumidores y usuarios serán sancionadas por los órganos correspondientes en materia de consumo.

Además, se incorpora una nueva redacción a la disposición adicional tercera de la mencionada Ley sobre el sistema arbitral de consumo en el sentido de que los prestadores y destinatarios de los servicios de la sociedad de la información pueden someter sus conflictos a este sistema de resolución.

Finalmente se revisa, actualiza y amplía el contenido de la actual disposición adicional quinta referida a la accesibilidad de las páginas de Internet, a fin de garantizar adecuadamente la accesibilidad para las personas con discapacidad y de edad avanzada a la información proporcionada por medios electrónicos.

IV

El artículo 5 de la Ley contempla las modificaciones necesarias en el articulado de la Ley 59/2003, de 19 de diciembre, de firma electrónica.

Estas modificaciones tienen por objeto clarificar las reglas de valoración de la firma electrónica en juicio y flexibilizar la obligación de los prestadores de servicios de certificación de comprobar los datos inscritos en registros públicos a fin de eliminar cargas excesivas.

El primer aspecto que se revisa del artículo 3 de la Ley de firma electrónica es la definición de «documento electrónico» que se modifica para alinearla en mayor medida con los conceptos utilizados en otras normas españolas de carácter general y en los países de nuestro entorno.

En segundo lugar, se aclara la redacción del apartado 8 del artículo 3, especificando que lo que debe comprobarse, en caso de impugnarse en juicio una firma electrónica reconocida, es si concurren los elementos constitutivos de dicho tipo de firma electrónica, es decir, que se trata de una firma electrónica avanzada basada en un certificado reconocido, que cumple todos los requisitos y condiciones establecidos en esta Ley para este tipo de certificados electrónicos, y que la firma se ha generado mediante un dispositivo seguro de creación de firma electrónica.

La tercera modificación acometida es la revisión de la regla de exención de responsabilidad establecida en el segundo inciso del apartado 5 del artículo 23 de la Ley que resulta en exceso rígida y onerosa para los prestadores de servicios de certificación, por lo que se procede a su oportuna flexibilización.

En coherencia con la mencionada modificación del artículo 23, se corrige asimismo el artículo 13, previendo que para la comprobación de los datos relativos a las personas jurídicas y a la representación de las mismas será suficiente que sean aportados y cotejados los documentos públicos en los que figuren los citados datos, estableciendo así un nivel de exigencia equiparable al empleado por las propias Administraciones Públicas en el cotejo y bastanteo de ese tipo de datos.

Se introduce, además, una modificación técnica de la actual redacción del apartado 4 del artículo 31.

Por último, al igual que en el caso de la Ley 34/2002, de 11 de julio, de Servicios de Sociedad de la Información y del Comercio Electrónico, este artículo incorpora una

disposición adicional undécima a la Ley de Firma Electrónica sobre resolución de conflictos en el sentido de que los usuarios y prestadores de servicios de certificación podrán someter las desavenencias que se susciten entre los mismos al procedimiento arbitral.

V

El artículo 6 incluye un nuevo tipo de infracción en el artículo 64 de la Ley 7/1996, de 15 de enero, de Ordenación del Comercio Minorista, a fin de respaldar la nueva obligación de disponer de un medio de interlocución electrónica para la prestación de servicios al público de especial trascendencia económica establecido en el artículo 2 de la presente Ley.

El artículo 7 de la Ley, introduce una serie de modificaciones en la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.

La primera de estas modificaciones afecta al apartado primero del artículo 22 letras a) y c) cuya finalidad es asegurar el acceso a los servicios telefónicos y de Internet como servicio universal. Mediante la redacción de la letra a) del artículo 22 apartado 1 se garantiza que todos usuarios finales puedan obtener una conexión a la red pública desde una ubicación fija y acceder a la prestación de servicio telefónico. La conexión debe ofrecer al usuario la posibilidad de efectuar y recibir llamadas telefónicas y permitir comunicaciones de fax y datos de velocidad suficiente para acceder a Internet, debiendo permitir dicha conexión comunicaciones en banda ancha en los términos definidos por la normativa vigente.

La redacción de la letra c) del citado precepto, garantiza tanto la existencia de una oferta suficiente de teléfonos públicos de pago en todo el territorio nacional, que satisfaga la necesidades de los usuarios, en cobertura geográfica y en número de aparatos, la accesibilidad de dichos teléfonos por los usuarios con discapacidades, como la calidad de los servicios con la posibilidad de efectuar gratuitamente llamadas de emergencia y finalmente la existencia de una oferta suficiente de equipos terminales de acceso a Internet de banda ancha en los términos que establezca la legislación en vigor.

Con el fin de reforzar los derechos de los usuarios frente a los proveedores de redes y servicios de comunicaciones electrónicas, se modifican los artículos 53 y 54 de la Ley General de Telecomunicaciones, mediante la tipificación como infracción administrativa del incumplimiento por parte de los operadores de los derechos de los consumidores y usuarios en el ámbito de las telecomunicaciones.

Asimismo, se reestablece la exención de la antigua tasa por reserva de uso especial del espectro, a radioaficionados y usuarios de la Banda Ciudadana CB-27 que figuraba en la Ley 11/1998, de 24 de abril, General de Telecomunicaciones, para aquellos usuarios que a la fecha de devengo hubieran cumplido los 65 años de edad, así como a los beneficiarios de una pensión pública o que tengan reconocido un grado de minusvalía igual o superior al 33 por 100.

El artículo 8 establece un nuevo régimen aplicable a las tarifas por las tareas de asignación, renovación y otras operaciones registrales realizadas por la entidad pública empresarial Red.es en ejercicio de su función de Autoridad de Asignación de los nombres de dominio de Internet bajo el código de país correspondiente a España, que pasarán a tener la consideración de precio público. Con ello, se permite a la entidad pública empresarial Red.es comercializar los nombres de dominio «.es» en las mismas condiciones en las que se comercializan el resto de nombres de dominio genéricos y territoriales.

La disposición adicional primera prevé que la autoridad de asignación de los nombres de dominio de Internet bajo el código de país correspondiente a España («.es») adopte las medidas que sean necesarias para asegurar que puedan asignarse nombres de dominio que contengan caracteres propios de las lenguas oficiales de España distintos de los incluidos en el alfabeto inglés, como es la letra «ñ» o la «ç», en un plazo máximo de 3 meses desde la entrada en vigor de esta Ley.

La disposición adicional segunda prevé que el Gobierno, en colaboración con las Comunidades Autónomas, impulsará la extensión de la banda ancha con el fin de conseguir antes del 31 de diciembre de 2008, una cobertura de servicio universal de banda ancha, para todos los ciudadanos, independientemente del tipo de tecnología utilizada en su caso y su ubicación geográfica. La acción del Gobierno deberá dirigirse prioritariamente a las áreas en las que la acción de los mecanismos del mercado sea insuficiente.

Asimismo, se especifica que el Gobierno analizará de forma continua las diferentes opciones tecnológicas y las condiciones de provisión de servicios de acceso a Internet de banda ancha. Para ello, se colaborará con los diferentes sectores interesados a fin de que asesoren al Gobierno en la elaboración de un informe anual sobre la situación del uso de los servicios de acceso a Internet de banda ancha en España que tendrá carácter público y podrá incluir recomendaciones para acelerar el despliegue de estos servicios. Estos análisis e informes deberán elaborarse de forma territorializada por Comunidades autónomas, compartiéndose los datos en formato electrónico con las Administraciones que lo soliciten.

Por su parte, la disposición adicional tercera prevé que el Gobierno elabore en el plazo de seis meses un Plan para la mejora de los niveles de seguridad y confianza en Internet, que incluirá directrices y medidas para aumentar la seguridad frente a las amenazas de Internet y proteger la privacidad on line.

La disposición adicional cuarta se refiere a las funciones de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información y a los órganos estadísticos de las Comunidades Autónomas en materia de requerimientos de información para fines estadísticos y de análisis. A estos efectos se atribuye a la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información tanto la facultad de recabar de los agentes que operan en el sector de las tecnologías de la información y de la sociedad de la información en general la información necesaria para el ejercicio de sus funciones como la potestad de sancionar las infracciones consistentes en no facilitar al mismo la información requerida.

En la disposición adicional quinta se establece la obligación de que en la elaboración de los proyectos de obras de construcción de carreteras o de infraestructuras ferroviarias se prevea la instalación de canalizaciones para el despliegue de redes de comunicaciones electrónicas a lo largo de toda la longitud de las mismas y del equipamiento para asegurar la cobertura de comunicaciones móviles en todo su recorrido. Estas canalizaciones deberán ponerse a disposición de los operadores de redes y servicios de comunicaciones electrónicas interesados en condiciones equitativas, no discriminatorias, neutrales y orientadas a costes.

La disposición adicional sexta encomienda al Ministerio de Industria, Turismo y Comercio la función de mantener una base de datos actualizada y sectorializada como mínimo por ámbitos territoriales de Comunidad autónoma sobre el despliegue y cobertura de infraestructuras y servicios de comunicaciones electrónicas y de la sociedad de la información en España.

La disposición adicional séptima establece que la constitución de la Agencia Estatal de Radiocomunicaciones tendrá lugar en el momento que se señale en el Real Decreto de aprobación de su Estatuto.

La disposición adicional octava modifica el apartado 13 del artículo 48 de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones. La norma establece en

Barcelona la sede de la Comisión del Mercado de las Telecomunicaciones que dispondrá de patrimonio independiente del patrimonio del Estado. Con la introducción de esta disposición se otorga rango de ley al establecimiento de la sede de dicha Comisión.

Las disposiciones adicionales novena y décima modifican, respectivamente, la Ley 2/1995, de 23 de marzo, de Sociedades de Responsabilidad Limitada y el texto refundido de la Ley de Sociedades Anónimas, aprobado por el Real Decreto Legislativo 1564/1989, de 22 de diciembre al objeto de rebajar de manera drástica los tiempos de constitución de una sociedad limitada pudiéndose reducir hasta cuatro días.

En concreto, la modificación se basa en las siguientes medidas: (i) Introducción de un modelo tipo u orientativo de estatutos en la sociedad de responsabilidad limitada; (ii) agilización de los trámites que implican la obtención de una denominación social como paso previo a la constitución de una sociedad de responsabilidad limitada, sin por ello restar importancia a la seguridad que aporta al tráfico mercantil el sistema vigente de denominaciones sociales, tutelado por el Registro Mercantil Central; y (iii) facultar a los administradores, desde el otorgamiento de la escritura fundacional, para el desarrollo del objeto social y para la realización de toda clase de actos y contratos relacionados con el mismo.

Esta disposición ha sido sometida al procedimiento de información en materia de normas y reglamentaciones técnicas previsto en la Directiva 98/34/CE, del Parlamento Europeo y del Consejo, de 22 de junio de 1998, por la que se establece un procedimiento de información en materia de normas y reglamentaciones técnicas, modificada por la Directiva 98/48/CE, del Parlamento Europeo y del Consejo, de 20 de julio de 1998, y en el Real Decreto 1337/1999, de 31 de julio, por el que se regula la remisión de información en materia de normas y reglamentaciones técnicas y reglamentos relativos a los servicios de la sociedad de la información.

La disposición adicional undécima introduce un aspecto de significativa relevancia ya que mandata a las Administraciones Públicas a promover el impulso, el desarrollo y la aplicación de los estándares de accesibilidad para las personas con discapacidad en los diseños y procesos basados en las nuevas tecnologías de la sociedad de la información.

Para garantizar el derecho de los ciudadanos a la utilización de las distintas lenguas del Estado, la disposición adicional duodécima impone a las Administraciones Públicas el deber de fomentar el pluralismo lingüístico en la sociedad de la información y la decimotercera establece, con el fin de impulsar los medios electrónicos propios de estas tecnologías, la obligación de regular los instrumentos telemáticos necesarios para ser utilizados por aquellos profesionales colegiados que elaboren y preparen proyectos e informes que hayan de incorporarse a los procedimientos que tramiten las Administraciones Públicas.

La disposición adicional decimocuarta atribuye al Centro Nacional de Referencia de Aplicación de las Tecnologías de Información y Comunicación (CENATIC), en colaboración con los Centros Autónomos de referencia y con el Centro de Transferencia de Tecnología entre Administraciones Públicas de la Administración General del Estado la difusión de las aplicaciones declaradas de fuente abierta por las propias Administraciones Públicas. Igualmente, el CENATIC se encargará del asesoramiento sobre los aspectos jurídicos, tecnológicos y metodológicos para la liberación del software y conocimiento.

Con objeto de fomentar la participación de la sociedad y de las entidades privadas sin ánimo de lucro y garantizar el pluralismo y la libertad de expresión en la sociedad de la información, la Ley incluye una disposición adicional decimoquinta en cuya virtud se establecerán los medios de apoyo y líneas de financiación para el desarrollo de los servicios de la sociedad de la información promovidos por estas entidades y que fomenten los valores democráticos, la participación ciudadana y atiendan al interés general o presten servicios a grupos sociales desfavorecidos.

La disposición adicional decimosexta se refiere a la puesta a disposición de los ciudadanos, en los términos legalmente establecidos de los contenidos digitales de las Administraciones Públicas de cuyos derechos de propiedad intelectual sean titulares o pertenezcan al dominio público.

La disposición adicional decimoséptima ofrece la posibilidad tanto a las personas físicas como jurídicas de poner a disposición del público los contenidos de las obras digitalizadas de las que sean titulares, con la finalidad de fomentar las nuevas tecnologías y la sociedad de la información entre los ciudadanos.

CAPÍTULO I

Medidas de impulso de la sociedad de la información

Artículo 1. *Medidas de impulso de la factura electrónica y del uso de medios electrónicos en otras fases de los procesos de contratación.*

1. La facturación electrónica en el marco de la contratación con el sector público estatal será obligatoria en los términos que se establezcan en la Ley reguladora de la contratación en el sector público y en su normativa de desarrollo.

A estos efectos, se entenderá que la factura electrónica es un documento electrónico que cumple con los requisitos legal y reglamentariamente exigibles a las facturas y que, además, garantiza la autenticidad de su origen y la integridad de su contenido, lo que impide el repudio de la factura por su emisor.

2. El Gobierno determinará el órgano competente de la Administración General del Estado que impulsará el empleo de la factura electrónica entre empresarios, profesionales y demás agentes del mercado, en particular, entre las pequeñas y medianas empresas y en las denominadas microempresas, con el fin de fomentar el desarrollo del comercio electrónico. Las Comunidades Autónomas, de acuerdo con las competencias que tengan reconocidas por sus Estatutos, colaborarán en coordinación con la Administración del Estado en el impulso del empleo de la factura electrónica.

El Gobierno, o en su caso las Comunidades Autónomas en el ámbito de sus competencias, establecerán, en un plazo máximo de nueve meses desde la entrada en vigor de esta Ley –o en el plazo que en su lugar establezca la Administración competente–, en coordinación con las Comunidades Autónomas –cuando no les corresponda la elaboración propia– y previa consulta a las asociaciones relevantes representativas de las entidades proveedoras de soluciones técnicas de facturación electrónica, a las asociaciones relevantes de usuarios de las mismas y a los colegios profesionales que agrupen a técnicos del sector de la Sociedad de la Información y de las Telecomunicaciones, un plan para la generalización del uso de la factura electrónica en España.

El citado Plan contendrá, entre otros, los criterios de accesibilidad y promoverá la interoperabilidad de las distintas soluciones de facturación electrónica. El Plan de la Administración General del Estado establecerá esquemas específicos de ayudas económicas para la implantación de la factura electrónica, en los cuales se contemplarán unos fondos generales para las Comunidades Autónomas que desarrollen su propio Plan para la generalización del uso de la factura electrónica, y serán estas últimas las que precisarán los destinos y condiciones de tramitación y concesión de las ayudas derivadas de estos fondos.

3. Los Ministerios de Industria, Turismo y Comercio y de Economía y Hacienda, teniendo en cuenta las compe-

tencias reconocidas a las Comunidades Autónomas, aprobarán, en un plazo máximo de 6 meses desde la entrada en vigor de esta Ley, las normas sobre formatos estructurados estándar de facturas electrónicas que sean necesarias para facilitar la interoperabilidad del sector público con el sector privado y favorecer y potenciar el tratamiento automatizado de las mismas. Estas normas no serán restrictivas y fomentarán que el sector público adopte los formatos de amplia implantación definidos por las organizaciones de estandarización globales pertinentes.

Los formatos estructurados de las facturas electrónicas permitirán su visualización y emisión en las distintas lenguas oficiales existentes, con la finalidad de garantizar los derechos de los usuarios.

4. Además, las diversas Administraciones Públicas promoverán en el ámbito de sus competencias y según su criterio la incorporación de la factura electrónica en las diferentes actuaciones públicas distintas de la contratación, en particular, en materia de justificación de ayudas y subvenciones.

5. Será de aplicación al tratamiento y conservación de los datos necesarios para la facturación electrónica lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal y sus normas de desarrollo.

Artículo 2. *Obligación de disponer de un medio de interlocución telemática para la prestación de servicios al público de especial trascendencia económica.*

1. Sin perjuicio de la utilización de otros medios de comunicación a distancia con los clientes, las empresas que presten servicios al público en general de especial trascendencia económica deberán facilitar a sus usuarios un medio de interlocución telemática que, mediante el uso de certificados reconocidos de firma electrónica, les permita la realización de, al menos, los siguientes trámites:

a) Contratación electrónica de servicios, suministros y bienes, la modificación y finalización o rescisión de los correspondientes contratos, así como cualquier acto o negocio jurídico entre las partes, sin perjuicio de lo establecido en la normativa sectorial.

b) Consulta de sus datos de cliente, que incluirán información sobre su historial de facturación de, al menos, los últimos tres años y el contrato suscrito, incluidas las condiciones generales si las hubiere.

c) Presentación de quejas, incidencias, sugerencias y, en su caso, reclamaciones, garantizando la constancia de su presentación para el consumidor y asegurando una atención personal directa.

d) Ejercicio de sus derechos de acceso, rectificación, cancelación y oposición en los términos previstos en la normativa reguladora de protección de datos de carácter personal.

2. A los efectos de lo dispuesto en el apartado anterior, tendrán la consideración de empresas que presten servicios al público en general de especial trascendencia económica, las que agrupen a más de cien trabajadores o su volumen anual de operaciones, calculado conforme a lo establecido en la normativa del Impuesto sobre el Valor Añadido, exceda de 6.010.121,04 euros y que, en ambos casos, operen en los siguientes sectores económicos:

a) Servicios de comunicaciones electrónicas a consumidores, en los términos definidos en la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.

b) Servicios financieros destinados a consumidores, que incluirán los servicios bancarios, de crédito o de pago, los servicios de inversión, las operaciones de seguros privados, los planes de pensiones y la actividad de mediación de seguros. En particular, se entenderá por:

1. Servicios bancarios, de crédito o de pago: las actividades relacionadas en el artículo 52 de la Ley 26/1988, de 29 de julio, sobre Disciplina e Intervención de las Entidades de Crédito.

2. Servicios de inversión: los definidos como tales en la Ley 24/1988, de 28 de julio, del Mercado de Valores.

3. Operaciones de seguros privados: las definidas en el artículo 3 del texto refundido de la Ley de ordenación y supervisión de los seguros privados, aprobado por Real Decreto Legislativo 6/2004, de 29 de octubre.

4. Planes de pensiones: los definidos en el artículo 1 del texto refundido de la Ley de Regulación de los Planes y Fondos de Pensiones, aprobado por Real Decreto Legislativo 1/2002, de 29 de noviembre.

5. Actividad de corredor de seguros: la definida en la Ley 26/2006, de 17 de julio, de mediación en seguros y reaseguros privados.

c) Servicios de suministro de agua a consumidores, definidos de acuerdo con la normativa específica.

d) Servicios de suministro de gas al por menor, de acuerdo con lo dispuesto en la Ley 34/1998, de 7 de octubre, del Sector de Hidrocarburos.

e) Servicios de suministro eléctrico a consumidores finales, de acuerdo con lo dispuesto en el título VIII de la Ley 54/1997, de 27 noviembre, del Sector Eléctrico.

f) Servicios de agencia de viajes, de acuerdo con lo dispuesto en el Real Decreto 271/1988, de 25 de marzo, por el que se regula el ejercicio de las actividades propias de las agencias de viajes.

g) Servicios de transporte de viajeros por carretera, ferrocarril, por vía marítima, o por vía aérea, de acuerdo con lo dispuesto en la normativa específica aplicable.

h) Actividades de comercio al por menor, en los términos fijados en el apartado 2 del artículo 1 de la Ley 7/1996, de 15 de enero, de ordenación del comercio minorista y en su normativa de desarrollo, a las que serán de aplicación únicamente los apartados c) y d) del apartado 1 del presente artículo.

3. Excepcionalmente, el Gobierno o, en su caso, los órganos competentes de las Comunidades Autónomas podrán ampliar el ámbito de aplicación del apartado 1 del presente artículo a otras empresas diferentes de las previstas en la Ley, en aquellos casos en los que, por la naturaleza del servicio que presten, se considere que en el desarrollo de su actividad normal deban tener una interlocución telemática con sus clientes o usuarios.

En el plazo de un año desde la entrada en vigor de la obligación a que se refiere el apartado 1, el Gobierno analizará la aplicación del apartado 2 de este artículo a otras empresas con más de cien trabajadores o que tengan un volumen anual de operaciones, calculado conforme a lo establecido en la normativa del Impuesto sobre el Valor Añadido, superior a 6.010.212,04 euros, que en el desarrollo de su actividad normal, presten servicios en los que se considere que deban tener una interlocución telemática con sus clientes o usuarios.

Las Comunidades Autónomas con competencias exclusivas en las materias objeto de obligación de comunicación telemática podrán modificar el ámbito y la intensidad de aplicación del apartado 1 del presente artículo en aquellos casos en que precisamente debido al desarrollo sectorial de sus competencias lo consideren oportuno.

Artículo 3. *Ofertas públicas de contratación electrónica entre empresas.*

1. A los efectos de este precepto se entiende por oferta pública de contratación electrónica entre empresas, aquel servicio de la sociedad de la información que consiste en un proceso enteramente electrónico abierto y limitado en el tiempo, por el que una empresa ofrece la

posibilidad de comprar o vender un determinado tipo de productos a otras empresas de manera que la contratación final se adjudique a la propuesta mejor valorada.

2. Las ofertas públicas de contratación electrónica entre empresas que se adscriban al protocolo de transparencia descrito en el apartado 3 de este artículo podrán ostentar la denominación de «Oferta pública de contratación electrónica de transparencia garantizada».

3. Para que una oferta pública de contratación electrónica entre empresas sea calificada de «Oferta pública de contratación electrónica de transparencia garantizada» deberá responder a los siguientes requisitos mínimos:

a) La empresa adjudicadora que decida recurrir a una oferta pública de contratación electrónica hará mención de ello en el anuncio de licitación que se publicará en la página corporativa de la empresa de forma accesible y visible para el conjunto de las empresas o para algunas previamente seleccionadas.

En el anuncio de licitación se invitará a presentar ofertas en un plazo razonable a partir de la fecha de publicación del anuncio.

b) Las condiciones de la empresa adjudicadora incluirán, al menos, información sobre los elementos a cuyos valores se refiere la oferta de pública de contratación electrónica, siempre que sean cuantificables y puedan ser expresados en cifras o porcentajes; en su caso, los límites de los valores que podrán presentarse, tal como resultan de las especificaciones del objeto del contrato; la información que se pondrá a disposición de los licitadores durante la oferta pública de contratación electrónica y el momento en que, en su caso, dispondrán de dicha información; la información pertinente sobre el desarrollo de la oferta pública de contratación electrónica; las condiciones en las que los licitadores podrán pujar, y, en particular, las diferencias mínimas que se exigirán, en su caso, para pujar; la información pertinente sobre el dispositivo electrónico utilizado y sobre las modalidades y especificaciones técnicas de conexión.

c) A lo largo del proceso de la oferta pública de contratación electrónica, la empresa adjudicadora comunicará a todos los licitadores como mínimo la información que les permita conocer en todo momento su respectiva clasificación. La empresa adjudicadora podrá, asimismo, comunicar otros datos relativos a otros precios o valores presentados. Los participantes únicamente podrán utilizar la información a la que se refiere este párrafo a fin de conocer su clasificación, sin que puedan proceder a su tratamiento para otra finalidad distinta de la señalada.

d) La empresa adjudicadora cerrará la oferta pública de contratación electrónica de conformidad con la fecha y hora fijadas previamente en el anuncio de licitación de la oferta pública de contratación.

e) Una vez concluido el proceso, la empresa informará a los participantes de la decisión adoptada.

4. El Gobierno promoverá que las empresas se adhieran a la calificación de «Oferta pública de contratación electrónica de transparencia garantizada» en sus relaciones comerciales.

CAPÍTULO II

Modificaciones legislativas para el impulso de la sociedad de la información y de las comunicaciones electrónicas

Artículo 4. *Modificaciones de la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico.*

Se modifica la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico, en los siguientes aspectos:

Uno. Se da nueva redacción al párrafo primero del artículo 4, con el texto siguiente:

«A los prestadores establecidos en países que no sean miembros de la Unión Europea o del Espacio Económico Europeo, les será de aplicación lo dispuesto en los artículos 7.2 y 11.2.»

Dos. Se da nueva redacción al artículo 8, con el texto siguiente:

«Artículo 8. *Restricciones a la prestación de servicios y procedimiento de cooperación intracomunitario.*

1. En caso de que un determinado servicio de la sociedad de la información atente o pueda atentar contra los principios que se expresan a continuación, los órganos competentes para su protección, en ejercicio de las funciones que tengan legalmente atribuidas, podrán adoptar las medidas necesarias para que se interrumpa su prestación o para retirar los datos que los vulneran. Los principios a que alude este apartado son los siguientes:

a) La salvaguarda del orden público, la investigación penal, la seguridad pública y la defensa nacional.

b) La protección de la salud pública o de las personas físicas o jurídicas que tengan la condición de consumidores o usuarios, incluso cuando actúen como inversores.

c) El respeto a la dignidad de la persona y al principio de no discriminación por motivos de raza, sexo, religión, opinión, nacionalidad, discapacidad o cualquier otra circunstancia personal o social, y

d) La protección de la juventud y de la infancia.

En la adopción y cumplimiento de las medidas de restricción a que alude este apartado se respetarán, en todo caso, las garantías, normas y procedimientos previstos en el ordenamiento jurídico para proteger los derechos a la intimidad personal y familiar, a la protección de los datos personales, a la libertad de expresión o a la libertad de información, cuando estos pudieran resultar afectados.

En todos los casos en los que la Constitución y las leyes reguladoras de los respectivos derechos y libertades así lo prevean de forma excluyente, sólo la autoridad judicial competente podrá adoptar las medidas previstas en este artículo, en tanto garante del derecho a la libertad de expresión, del derecho de producción y creación literaria, artística, científica y técnica, la libertad de cátedra y el derecho de información.

2. La adopción de restricciones a la prestación de servicios de la sociedad de la información provenientes de prestadores establecidos en un Estado de la Unión Europea o del Espacio Económico Europeo distinto a España deberá seguir el procedimiento de cooperación intracomunitario descrito en el siguiente apartado de este artículo, sin perjuicio de lo dispuesto en la legislación procesal y de cooperación judicial.

3. Cuando un órgano competente acuerde, en ejercicio de las competencias que tenga legalmente atribuidas, y de acuerdo con lo dispuesto en el párrafo a) del apartado 4 del artículo 3 de la Directiva 2000/31/CE, establecer restricciones que afecten a un servicio de la sociedad de la información que proceda de alguno de los Estados miembros de la Unión Europea o del Espacio Económico Europeo distinto de España, dicho órgano deberá seguir el siguiente procedimiento:

a) El órgano competente requerirá al Estado miembro en que esté establecido el prestador afectado para que adopte las medidas oportunas. En el caso de que no las adopte o resulten insuficientes, dicho órgano notificará, con carácter previo, a la Comisión Europea o, en su caso, al Comité Mixto del Espacio Económico Europeo y al Estado miembro de que se trate las medidas que tiene intención de adoptar.

b) En los supuestos de urgencia, el órgano competente podrá adoptar las medidas oportunas, notificándolas al Estado miembro de procedencia y a la Comisión Europea o, en su caso, al Comité Mixto del Espacio Económico Europeo con la mayor brevedad y, en cualquier caso, como máximo, en el plazo de quince días desde su adopción. Así mismo, deberá indicar la causa de dicha urgencia.

Los requerimientos y notificaciones a que alude este apartado se realizarán siempre a través del órgano de la Administración General del Estado competente para la comunicación y transmisión de información a las Comunidades Europeas.

4. Los órganos competentes de otros Estados Miembros de la Unión Europea o del Espacio Económico Europeo podrán requerir la colaboración de los prestadores de servicios de intermediación establecidos en España en los términos previstos en el apartado 2 del artículo 11 de esta ley si lo estiman necesario para garantizar la eficacia de las medidas de restricción que adopten al amparo del apartado anterior.

5. Las medidas de restricción que se adopten al amparo de este artículo deberán, en todo caso, cumplir las garantías y los requisitos previstos en los apartados 3 y 4 del artículo 11 de esta ley.»

Tres. Se suprime el artículo 9, sobre constancia registral del nombre de dominio, que queda sin contenido.

Cuatro. Se da nueva redacción a los párrafos b) y f) del apartado 1 del artículo 10, con el texto siguiente:

«b) Los datos de su inscripción en el Registro Mercantil en el que, en su caso, se encuentren inscritos o de aquel otro registro público en el que lo estuvieran para la adquisición de personalidad jurídica o a los solos efectos de publicidad.»

«f) Cuando el servicio de la sociedad de la información haga referencia a precios, se facilitará información clara y exacta sobre el precio del producto o servicio, indicando si incluye o no los impuestos aplicables y, en su caso, sobre los gastos de envío o en su caso aquello que dispongan las normas de las Comunidades Autónomas con competencias en la materia.»

Cinco. Se da nueva redacción al artículo 11, con el texto siguiente:

«Artículo 11. *Deber de colaboración de los prestadores de servicios de intermediación.*

1. Cuando un órgano competente hubiera ordenado, en ejercicio de las competencias que legalmente tenga atribuidas, que se interrumpa la prestación de un servicio de la sociedad de la información o la retirada de determinados contenidos provenientes de prestadores establecidos en España, y para ello fuera necesaria la colaboración de los prestadores de servicios de intermediación, dicho órgano podrá ordenar a los citados prestadores que suspendan el correspondiente servicio de intermediación utilizado para la provisión del servicio de la sociedad de la información o de los contenidos cuya interrupción o retirada hayan sido ordenados respectivamente.

2. Si para garantizar la efectividad de la resolución que acuerde la interrupción de la prestación de un servicio o la retirada de contenidos procedentes de un prestador establecido en un Estado no perteneciente a la Unión Europea o al Espacio Económico Europeo, el órgano competente estimara necesario impedir el acceso desde España a los mismos, y para ello fuera necesaria la colaboración de los prestadores de servicios de intermediación establecidos en España, dicho órgano podrá ordenar a los citados prestadores de servicios de intermediación que suspendan el correspondiente servicio de intermediación utilizado para la provisión del servicio de la sociedad de la información o de los contenidos cuya interrupción o retirada hayan sido ordenados respectivamente.

3. En la adopción y cumplimiento de las medidas a que se refieren los apartados anteriores, se respetarán, en todo caso, las garantías, normas y procedimientos previstos en el ordenamiento jurídico para proteger los derechos a la intimidad personal y familiar, a la protección de los datos personales, a la libertad de expresión o a la libertad de información, cuando estos pudieran resultar afectados.

En todos los casos en que la Constitución, las normas reguladoras de los respectivos derechos y libertades o las que resulten aplicables a las diferentes materias atribuyan competencia a los órganos jurisdiccionales de forma excluyente para intervenir en el ejercicio de actividades o derechos, sólo la autoridad judicial competente podrá adoptar las medidas previstas en este artículo. En particular, la autorización del secuestro de páginas de Internet o de su restricción cuando ésta afecte a los derechos y libertades de expresión e información y demás amparados en los términos establecidos en el artículo 20 de la Constitución solo podrá ser decidida por los órganos jurisdiccionales competentes.

4. Las medidas a que hace referencia este artículo serán objetivas, proporcionadas y no discriminatorias, y se adoptarán de forma cautelar o en ejecución de las resoluciones que se dicten, conforme a los procedimientos administrativos legalmente establecidos o a los previstos en la legislación procesal que corresponda.»

Seis. Se incluye un nuevo artículo 12 bis, con la siguiente redacción:

«Artículo 12 bis. *Obligaciones de información sobre seguridad.*

1. Los proveedores de servicios de intermediación establecidos en España de acuerdo con lo dispuesto en el artículo 2 de esta Ley que realicen actividades consistentes en la prestación de servicios de acceso a Internet, estarán obligados a informar a sus clientes de forma permanente, fácil, directa y gratuita, sobre los diferentes medios de carácter técnico que aumenten los niveles de la seguridad de la información y permitan, entre otros, la protección frente a virus informáticos y programas espía, y la restricción de los correos electrónicos no solicitados.

2. Los proveedores de servicios de acceso a Internet y los prestadores de servicios de correo electrónico o de servicios similares deberán informar a sus clientes de forma permanente, fácil, directa y gratuita sobre las medidas de seguridad que apliquen en la provisión de los mencionados servicios.

3. Igualmente, los proveedores de servicios referidos en el apartado 1 informarán sobre las herramientas existentes para el filtrado y restricción del acceso a determinados contenidos y servicios en Internet no deseados o que puedan resultar nocivos para la juventud y la infancia.

4. Los proveedores de servicios mencionados en el apartado 1 facilitarán información a sus clientes acerca de las posibles responsabilidades en que puedan incurrir por el uso de Internet con fines ilícitos, en particular, para la comisión de ilícitos penales y por la vulneración de la legislación en materia de propiedad intelectual e industrial.

5. Las obligaciones de información referidas en los apartados anteriores se darán por cumplidas si el correspondiente proveedor incluye la información exigida en su página o sitio principal de Internet en la forma establecida en los mencionados apartados.»

Siete. Se da nueva redacción al apartado 2 del artículo 17, con el texto siguiente:

«2. La exención de responsabilidad establecida en el apartado 1 no operará en el supuesto de que el proveedor de contenidos al que se enlace o cuya localización se facilite actúe bajo la dirección, autoridad o control del prestador que facilite la localización de esos contenidos.»

Ocho. Se modifica el apartado 3 del artículo 18, teniendo éste el siguiente tenor literal:

«3. Los códigos de conducta a los que hacen referencia los apartados precedentes deberán ser accesibles por vía electrónica. Se fomentará su traducción a otras lenguas oficiales, en el Estado y de la Unión Europea, con objeto de darles mayor difusión.»

Nueve. Se da nueva redacción al artículo 20, con el texto siguiente:

«Artículo 20. *Información exigida sobre las comunicaciones comerciales, ofertas promocionales y concursos.*

1. Las comunicaciones comerciales realizadas por vía electrónica deberán ser claramente identificables como tales y la persona física o jurídica en nombre de la cual se realizan también deberá ser claramente identificable.

En el caso en el que tengan lugar a través de correo electrónico u otro medio de comunicación electrónica equivalente incluirán al comienzo del mensaje la palabra "publicidad" o la abreviatura "publi".

2. En los supuestos de ofertas promocionales, como las que incluyan descuentos, premios y regalos, y de concursos o juegos promocionales, previa la correspondiente autorización, se deberá asegurar, además del cumplimiento de los requisitos establecidos en el apartado anterior y en las normas de ordenación del comercio, que queden claramente identificados como tales y que las condiciones de acceso y, en su caso, de participación sean fácilmente accesibles y se expresen de forma clara e inequívoca.

3. Lo dispuesto en los apartados anteriores se entiende sin perjuicio de lo que dispongan las normativas dictadas por las Comunidades Autónomas con competencias exclusivas sobre consumo, comercio electrónico o publicidad.»

Diez. Se da nueva redacción al apartado 1 del artículo 24, con el texto siguiente:

«1. La prueba de la celebración de un contrato por vía electrónica y la de las obligaciones que tienen su origen en él se sujetará a las reglas generales del ordenamiento jurídico.

Cuando los contratos celebrados por vía electrónica estén firmados electrónicamente se estará a lo establecido en el artículo 3 de la Ley 59/2003, de 19 de diciembre, de firma electrónica.»

Once. Se da nueva redacción a la rúbrica y a los apartados 1 y 2 del artículo 27, con el texto siguiente:

«Artículo 27. *Obligaciones previas a la contratación.*

1. Además del cumplimiento de los requisitos en materia de información que se establecen en la normativa vigente, el prestador de servicios de la sociedad de la información que realice actividades de contratación electrónica tendrá la obligación de poner a disposición del destinatario, antes de iniciar el procedimiento de contratación y mediante técnicas adecuadas al medio de comunicación utilizado, de forma permanente, fácil y gratuita, información clara, comprensible e inequívoca sobre los siguientes extremos:

a) Los distintos trámites que deben seguirse para celebrar el contrato.

b) Si el prestador va a archivar el documento electrónico en que se formalice el contrato y si éste va a ser accesible.

c) Los medios técnicos que pone a su disposición para identificar y corregir errores en la introducción de los datos, y

d) La lengua o lenguas en que podrá formalizarse el contrato.

La obligación de poner a disposición del destinatario la información referida en el párrafo anterior se dará por cumplida si el prestador la incluye en su página o sitio de Internet en las condiciones señaladas en dicho párrafo.

Cuando el prestador diseñe específicamente sus servicios de contratación electrónica para ser accedidos mediante dispositivos que cuenten con pantallas de formato reducido, se entenderá cumplida la obligación establecida en este apartado cuando facilite de manera permanente, fácil, directa y exacta la dirección de Internet en que dicha información es puesta a disposición del destinatario.

2. El prestador no tendrá la obligación de facilitar la información señalada en el apartado anterior cuando:

a) Ambos contratantes así lo acuerden y ninguno de ellos tenga la consideración de consumidor, o

b) El contrato se haya celebrado exclusivamente mediante intercambio de correo electrónico u otro tipo de comunicación electrónica equivalente.»

Doce. Se da una nueva redacción al artículo 33, con el siguiente texto:

«Los destinatarios y prestadores de servicios de la sociedad de la información podrán dirigirse a cualesquiera órganos competentes en materia de sociedad de la información, sanidad y consumo de las Administraciones Públicas, para:

a) Conseguir información general sobre sus derechos y obligaciones contractuales en el marco de la normativa aplicable a la contratación electrónica,

b) Informarse sobre los procedimientos de resolución judicial y extrajudicial de conflictos, y

c) Obtener los datos de las autoridades, asociaciones u organizaciones que puedan facilitarles información adicional o asistencia práctica.

La comunicación con dichos órganos podrá hacerse por medios electrónicos.»

Trece. Se da una nueva redacción a los apartados 1 y 2 del artículo 35, con el texto siguiente:

«1. El Ministerio de Industria, Turismo y Comercio en el ámbito de la Administración General del Estado, y los órganos que correspondan de las Comunidades Autónomas, controlarán, en sus respectivos ámbitos territoriales y competenciales, el cumplimiento por los prestadores de servicios de la sociedad de la información de las obligaciones establecidas en esta Ley y en sus disposiciones de desarrollo, en lo que se refiere a los servicios propios de la sociedad de la información.

No obstante, las referencias a los órganos competentes contenidas en los artículos 8, 10, 11, 15, 16, 17 y 38 se entenderán hechas a los órganos jurisdiccionales o administrativos que, en cada caso, lo sean en función de la materia.

2. Los órganos citados en el apartado 1 de este artículo podrán realizar las actuaciones inspectoras que sean precisas para el ejercicio de su función de control.

Los funcionarios adscritos a dichos órganos y que ejerzan la inspección a que se refiere el párrafo anterior tendrán la consideración de autoridad pública en el desempeño de sus cometidos.»

Catorce. Se suprime la letra a) del apartado 2 del artículo 38 que queda sin contenido.

Quince. Se da nueva redacción a la letra a) del apartado 4 del artículo 38, con el texto siguiente:

«a) El incumplimiento de lo previsto en el artículo 12 bis.»

Dieciséis. Se da una nueva redacción al artículo 43, con el siguiente texto:

«1. La imposición de sanciones por incumplimiento de lo previsto en esta Ley corresponderá al órgano o autoridad que dictó la resolución incumplida o al que estén adscritos los inspectores. Asimismo las infracciones respecto a los derechos y garantías de los consumidores y usuarios serán sancionadas por el órgano correspondiente de las Comunidades Autónomas competentes en materia de consumo.

2. En la Administración General del Estado, la imposición de sanciones por el incumplimiento de lo previsto en esta Ley corresponderá, en el caso de infracciones muy graves, al Ministro de Industria, Turismo y Comercio, y en el de infracciones graves y leves, al Secretario de Estado de Telecomunicaciones y para la Sociedad de la Información.

No obstante lo anterior, la imposición de sanciones por incumplimiento de las resoluciones dictadas por los órganos competentes en función de la materia o entidad de que se trate a que se refieren los párrafos a) y b) del artículo 38.2 de esta Ley corresponderá al órgano que dictó la resolución incumplida. Igualmente, corresponderá a la Agencia de Protección de Datos la imposición de sanciones por la comisión de las infracciones tipificadas en los artículos 38.3 c), d) e i) y 38.4 d), g) y h) de esta Ley.

3. La potestad sancionadora regulada en esta Ley se ejercerá de conformidad con lo establecido al respecto en la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, y en sus normas de desarrollo. No obstante, el plazo máximo de duración del procedimiento simplificado será de tres meses.»

Diecisiete. Se da una nueva redacción a la disposición adicional tercera, con el texto siguiente:

«Disposición adicional tercera. *Sistema Arbitral de Consumo.*

El prestador y el destinatario de servicios de la sociedad de la información podrán someter sus conflictos al arbitraje de consumo, mediante la adhesión de aquéllos al Sistema Arbitral de Consumo competente que se prestará también por medios electrónicos, conforme al procedimiento establecido reglamentariamente.»

Dieciocho. Se da nueva redacción al párrafo segundo del apartado uno de la disposición adicional quinta, con el texto siguiente:

«A partir del 31 de diciembre de 2008, las páginas de Internet de las Administraciones Públicas satisfarán, como mínimo, el nivel medio de los criterios de accesibilidad al contenido generalmente reconocidos. Excepcionalmente, esta obligación no será aplicable cuando una funcionalidad o servicio no disponga de una solución tecnológica que permita su accesibilidad.»

Diecinueve. Se añaden dos nuevos párrafos, que pasarán a ser respectivamente el tercero y el cuarto, al apartado uno de la disposición adicional quinta, con el texto siguiente:

«Las Administraciones Públicas exigirán que tanto las páginas de Internet cuyo diseño o mantenimiento financien total o parcialmente como las páginas de Internet de entidades y empresas que se encarguen de gestionar servicios públicos apliquen los criterios de accesibilidad antes mencionados. En particular, será obligatorio lo expresado en este apartado para las páginas de Internet y sus contenidos de los Centros públicos educativos, de formación y universitarios, así como, de los Centros privados que obtengan financiación pública.

Las páginas de Internet de las Administraciones Públicas deberán ofrecer al usuario información sobre su nivel de accesibilidad y facilitar un sistema de contacto para que puedan transmitir las dificultades de acceso al contenido de las páginas de Internet o formular cualquier queja, consulta o sugerencia de mejora.»

Veinte. Se añaden tres nuevos apartados, que pasarán a ser los apartados tres, cuatro y cinco, a la disposición adicional quinta, con el texto siguiente:

«Tres. Las Administraciones Públicas promoverán medidas de sensibilización, educación y formación sobre accesibilidad con objeto de promover que los titulares de otras páginas de Internet incorporen progresivamente los criterios de accesibilidad.

Cuatro. Los incumplimientos de las obligaciones de accesibilidad establecidas en esta Disposición adicional estarán sometidos al régimen de infracciones y sanciones vigente en materia de igualdad de oportunidades, no discriminación y accesibilidad universal de las personas con discapacidad.

Cinco. Las páginas de Internet de las empresas que presten servicios al público en general de especial trascendencia económica, sometidas a la obligación establecida en el artículo 2 de la Ley 56/2007, de medidas de impulso de la sociedad de la información, deberán satisfacer a partir del 31 de diciembre de 2008, como mínimo, el nivel medio de los criterios de accesibilidad al contenido generalmente reconocidos. Excepcionalmente, esta obligación no

será aplicable cuando una funcionalidad o servicio no disponga de una solución tecnológica que permita su accesibilidad.»

Artículo 5. *Modificaciones de la Ley 59/2003, de 19 de diciembre, de firma electrónica.*

Se modifica la Ley 59/2003, de 19 de diciembre, de firma electrónica, en los siguientes aspectos:

Uno. Se da nueva redacción al apartado 5 del artículo 3, con el texto siguiente:

«5. Se considera documento electrónico la información de cualquier naturaleza en forma electrónica, archivada en un soporte electrónico según un formato determinado y susceptible de identificación y tratamiento diferenciado.

Sin perjuicio de lo dispuesto en el párrafo anterior, para que un documento electrónico tenga la naturaleza de documento público o de documento administrativo deberá cumplirse, respectivamente, con lo dispuesto en las letras a) o b) del apartado siguiente y, en su caso, en la normativa específica aplicable.»

Dos. Se da nueva redacción al apartado 8 del artículo 3, con el texto siguiente:

«8. El soporte en que se hallen los datos firmados electrónicamente será admisible como prueba documental en juicio. Si se impugnare la autenticidad de la firma electrónica reconocida con la que se hayan firmado los datos incorporados al documento electrónico se procederá a comprobar que se trata de una firma electrónica avanzada basada en un certificado reconocido, que cumple todos los requisitos y condiciones establecidos en esta Ley para este tipo de certificados, así como que la firma se ha generado mediante un dispositivo seguro de creación de firma electrónica.

La carga de realizar las citadas comprobaciones corresponderá a quien haya presentado el documento electrónico firmado con firma electrónica reconocida. Si dichas comprobaciones obtienen un resultado positivo, se presumirá la autenticidad de la firma electrónica reconocida con la que se haya firmado dicho documento electrónico siendo las costas, gastos y derechos que origine la comprobación exclusivamente a cargo de quien hubiese formulado la impugnación. Si, a juicio del tribunal, la impugnación hubiese sido temeraria, podrá imponerle, además, una multa de 120 a 600 euros.

Si se impugna la autenticidad de la firma electrónica avanzada, con la que se hayan firmado los datos incorporados al documento electrónico, se estará a lo establecido en el apartado 2 del artículo 326 de la Ley de Enjuiciamiento Civil.»

Tres. Se da nueva redacción a los apartados 2 y 3 del artículo 13, con el texto siguiente:

«2. En el caso de certificados reconocidos de personas jurídicas, los prestadores de servicios de certificación comprobarán, además, los datos relativos a la constitución y personalidad jurídica y a la extensión y vigencia de las facultades de representación del solicitante mediante los documentos públicos que sirvan para acreditar los extremos citados de manera fehaciente y su inscripción en el correspondiente registro público si así resulta exigible. La citada comprobación podrá realizarse, asimismo, mediante consulta en el registro público en el que estén inscritos los documentos de constitución y d4e apoderamiento, pudiendo emplear los medios telemáticos facilitados por los citados registros públicos.

3. Si los certificados reconocidos reflejan una relación de representación voluntaria, los prestadores de servicios de certificación comprobarán los datos relativos a la personalidad jurídica del representado y a la extensión y vigencia de las facultades del representante mediante los documentos públicos que sirvan para acreditar los extremos citados de manera fehaciente y su inscripción en el correspondiente registro público si así resulta exigible. La citada comprobación podrá realizarse, asimismo, mediante consulta en el registro público en el que estén inscritos los mencionados datos, pudiendo emplear los medios telemáticos facilitados por los citados registros públicos.

Si los certificados reconocidos admiten otros supuestos de representación, los prestadores de servicios de certificación deberán exigir la acreditación de las circunstancias en las que se fundamenten, en la misma forma prevista anteriormente.

Cuando el certificado reconocido contenga otras circunstancias personales o atributos del solicitante, como su condición de titular de un cargo público, su pertenencia a un colegio profesional o su titulación, éstas deberán comprobarse mediante los documentos oficiales que las acrediten, de conformidad con su normativa específica.»

Cuatro. Se da nueva redacción al apartado 5 del artículo 23, con el texto siguiente:

«5. El prestador de servicios de certificación no será responsable de los daños y perjuicios ocasionados al firmante o terceros de buena fe por la inexactitud de los datos que consten en el certificado electrónico si éstos le han sido acreditados mediante documento público, inscrito en un registro público si así resulta exigible. En caso de que dichos datos deban figurar inscritos en un registro público, el prestador de servicios de certificación podrá, en su caso, comprobarlos en el citado registro antes de la expedición del certificado, pudiendo emplear los medios telemáticos facilitados por los citados registros públicos.»

Cinco. Se da nueva redacción al apartado 4 del artículo 31, con el texto siguiente:

«4. Constituyen infracciones leves:

El incumplimiento por los prestadores de servicios de certificación que no expidan certificados reconocidos de las obligaciones establecidas en el artículo 18; y el incumplimiento por los prestadores de servicios de certificación de las restantes obligaciones establecidas en esta Ley, cuando no constituya infracción grave o muy grave, con excepción de las obligaciones contenidas en el apartado 2 del artículo 30.»

Seis. Se añade una disposición adicional, con la siguiente redacción:

«Disposición adicional undécima. *Resolución de conflictos.*

Los usuarios y prestadores de servicios de certificación podrán someter los conflictos que se susciten en sus relaciones al arbitraje.

Cuando el usuario tenga la condición de consumidor o usuario, en los términos establecidos por la legislación de protección de los consumidores, el prestador y el usuario podrán someter sus conflictos al arbitraje de consumo, mediante la adhesión de aquéllos al Sistema Arbitral de Consumo competente.»

Artículo 6. *Modificación de la Ley 7/1996, de 15 de enero, de ordenación del comercio minorista.*

Se añade una nueva letra i) al artículo 64 de la Ley 7/1996, de 15 de enero, de ordenación del comercio minorista, con la siguiente redacción:

«i) Los incumplimientos de lo dispuesto en el párrafo d) del apartado 1 del citado artículo 2 serán sancionables conforme a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal correspondiendo la potestad sancionadora al órgano que resulte competente.»

Artículo 7. *Modificaciones de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.*

Se modifica la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, en los siguientes aspectos:

Uno. Se modifican las letras a) y c) del apartado 1 del artículo 22 quedando con la siguiente redacción:

«a) Que todos los usuarios finales puedan obtener una conexión a la red telefónica pública desde una ubicación fija y acceder a la prestación del servicio telefónico disponible al publico, siempre que sus solicitudes se consideren razonables en los términos que reglamentariamente se determinen. La conexión debe ofrecer al usuario final la posibilidad de efectuar y recibir llamadas telefónicas y permitir comunicaciones de fax y datos a velocidad suficiente para acceder de forma funcional a Internet. No obstante, la conexión deberá permitir comunicaciones en banda ancha, en los términos que se definan por la normativa vigente.»

«c) Que exista una oferta suficiente de teléfonos públicos de pago, en todo el territorio nacional, que satisfaga razonablemente las necesidades de los usuarios finales, en cobertura geográfica, en número de aparatos, accesibilidad de estos teléfonos por los usuarios con discapacidades y calidad de los servicios y, que sea posible efectuar gratuitamente llamadas de emergencia desde los teléfonos públicos de pago sin tener que utilizar ninguna forma de pago, utilizando el número único de llamadas de emergencia 112 y otros números de emergencia españoles. Asimismo, en los términos que se definan por la normativa vigente para el servicio universal, que exista una oferta suficiente de equipos terminales de acceso a Internet de banda ancha.»

Dos. Se introduce una nueva redacción en el apartado l) del artículo 53 que queda redactado de la siguiente forma:

«l) El incumplimiento grave o reiterado de las obligaciones de servicio público y la grave o reiterada vulneración de los derechos de los consumidores y usuarios finales según lo establecido en el Título III de la Ley y su normativa de desarrollo, con excepción de los establecidos por el artículo 38.3 cuya vulneración será sancionable conforme a lo previsto en el párrafo z) de este artículo.»

Tres. El apartado o) del artículo 54 queda redactado de la siguiente forma:

«o) El incumplimiento de las obligaciones de servicio público y la vulneración de los derechos de los consumidores y usuarios finales, según lo establecido en el Título III de la Ley y su normativa de desarrollo, salvo que deban considerarse como infracción muy grave, conforme a lo previsto en el artículo anterior.

No obstante, la vulneración de los derechos establecidos por el artículo 38.3 de esta Ley será sancionable conforme a lo previsto en el párrafo r) de este artículo.»

Cuatro. Se modifica el apartado 7 del punto 3 del Anexo I, que queda redactado como sigue:

«Las Administraciones Públicas estarán exentas del pago de esta tasa en los supuestos de reserva de dominio público radioeléctrico para la prestación de servicios obligatorios de interés general que tenga exclusivamente por objeto la defensa nacional, la seguridad pública y las emergencias, así como cualesquiera otros servicios obligatorios de interés general sin contrapartida económica directa o indirecta, como tasas, precios públicos o privados, ni otros ingresos derivados de dicha prestación, tales como los ingresos en concepto de publicidad. A tal efecto, deberán solicitar, fundamentadamente, dicha exención al Ministerio de Industria, Turismo y Comercio. Asimismo, no estarán sujetos al pago los enlaces descendentes de radiodifusión por satélite, tanto sonora como de televisión.»

Cinco. Se añade un nuevo apartado 5 al epígrafe 4 «Tasas de telecomunicaciones», del Anexo I «Tasas en materia de telecomunicaciones», con la siguiente redacción:

«5. Estarán exentos del pago de la tasa de tramitación de autorizaciones de uso especial de dominio público radioeléctrico aquellos solicitantes de dichas autorizaciones que cumplan 65 años en el año en que efectúen la solicitud, o que los hayan cumplido con anterioridad, así como los beneficiarios de una pensión pública o que tengan reconocido un grado de minusvalía igual o superior al 33 por 100.»

Artículo 8. *Modificación de los apartados 9 y 10 de la Disposición adicional sexta de la Ley 11/1998, de 24 de abril, General de Telecomunicaciones.*

Se modifican los apartados 9 y 10 de la Disposición adicional sexta de la Ley 11/1998, de 24 de abril, General de Telecomunicaciones, que quedarán redactados de la siguiente forma:

«9. Los recursos económicos de la entidad podrán provenir de cualquiera de los enumerados en el apartado 1 del artículo 65 de la Ley 6/1997, de 14 de abril, de Organización y Funcionamiento de la Administración General del Estado. Entre los recursos económicos de la entidad pública empresarial Red.es se incluyen los ingresos provenientes de lo recaudado en concepto del precio público por las operaciones de registro relativas a los nombres de dominio de Internet bajo el código de país correspondiente a España ".es" regulado en el apartado siguiente.

10. Precios Públicos por asignación, renovación y otras operaciones registrales de los nombres de dominio bajo el ".es".

La contraprestación pecuniaria que se satisfaga por la asignación, renovación y otras operaciones registrales realizadas por la entidad pública empresarial Red.es en ejercicio de su función de Autoridad de Asignación de los nombres de dominio de Internet bajo el código de país correspondiente a España tendrán la consideración de precio público.

Red.es, previa autorización del Ministerio de Industria, Turismo y Comercio, establecerá mediante

la correspondiente Instrucción, las tarifas de los precios públicos por la asignación, renovación y otras operaciones de registro de los nombres de dominio bajo el ".es". La propuesta de establecimiento o modificación de la cuantía de precios públicos irá acompañada, de conformidad con lo previsto en el artículo 26 de la Ley 8/1989, de 13 de abril, que regula el Régimen Jurídico de las Tasas y Precios Públicos, de una memoria económico-financiera que justificará el importe de los mismos que se proponga y el grado de cobertura financiera de los costes correspondientes.

La gestión recaudatoria de los precios públicos referidos en este apartado corresponde a la entidad pública empresarial Red.es que determinará el procedimiento para su liquidación y pago mediante la Instrucción mencionada en el párrafo anterior en la que se establecerán los modelos de declaración, plazos y formas de pago.

La entidad pública empresarial Red.es podrá exigir la anticipación o el depósito previo del importe total o parcial de los precios públicos por las operaciones de registro relativas a los nombres de dominio ".es".»

Disposición adicional primera. *Utilización de caracteres de las lenguas oficiales de España en el «.es».*

La autoridad de asignación de los nombres de dominio de Internet bajo el código de país correspondiente a España («.es») adoptará las medidas que sean necesarias para asegurar que puedan asignarse nombres de dominio que contengan caracteres propios de las lenguas oficiales de España distintos de los incluidos en el alfabeto inglés en un plazo máximo de 3 meses desde la entrada en vigor de esta Ley.

Con carácter previo a que los mecanismos de reconocimiento de caracteres multilingües estén disponibles para la asignación de nombres de dominio bajo el código de país «.es», la autoridad de asignación dará publicidad a la posibilidad de solicitar nombres de dominio que contengan dichos caracteres y establecerá con antelación suficiente un registro escalonado para los mismos. En este registro escalonado se dará preferencia a las solicitudes de nombres de dominio con caracteres multilingües que resulten equivalentes a nombres de dominio bajo el código de país «.es» previamente asignados, en los términos que determine la autoridad de asignación.

Disposición adicional segunda. *Extensión de servicios de acceso a banda ancha.*

El Gobierno, en colaboración con las Comunidades Autónomas, impulsará la extensión de la banda ancha con el fin de conseguir, antes del 31 de diciembre de 2008, una cobertura de servicio universal de conexión a banda ancha, para todos los ciudadanos, independientemente del tipo de tecnología utilizada en cada caso y de su ubicación geográfica.

El Gobierno analizará de manera continua y permanente las diferentes opciones tecnológicas y las condiciones de provisión de servicios de acceso a Internet de banda ancha para el conjunto de ciudadanos y empresas en España. En particular, se colaborará con los diferentes sectores relevantes interesados, a fin de que asesoren al Gobierno en la elaboración de un informe anual sobre la situación del uso de los servicios de acceso a Internet de banda ancha en España. Este informe será de carácter público y podrá elaborar recomendaciones para acelerar el despliegue de los citados servicios.

A efectos de realizar los análisis e informes mencionados en los párrafos anteriores el Ministerio de Industria, Turismo y Comercio podrá realizar los requerimientos de información generales o particularizados que sean necesarios en los términos previstos en la disposición adicional quinta de esta Ley.

Los análisis e informes mencionados deberán realizarse de forma territorializada por Comunidades Autónomas y se compartirán los datos en formato electrónico con las Administraciones que lo soliciten.

Disposición adicional tercera. *Plan de mejora de los niveles de seguridad y confianza en Internet.*

El Gobierno elaborará, en un plazo de seis meses, un Plan, tecnológicamente neutro, para la mejora de los niveles de seguridad y confianza en Internet, que incluirá directrices y medidas para aumentar la seguridad frente a las amenazas de Internet y proteger la privacidad on line. Este plan se revisará periódicamente para poder responder al escenario de amenazas en continua evolución.

Disposición adicional cuarta. *Requerimientos de información para fines estadísticos y de análisis.*

1. La Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, y los órganos estadísticos de las Comunidades Autónomas con competencias en materia de estadística, podrán requerir de los fabricantes de productos y proveedores de servicios referentes a las Tecnologías de la Información, a la Sociedad de la Información, a los contenidos digitales y al entretenimiento digital la información necesaria para el ejercicio de sus funciones para fines estadísticos y de análisis.

La Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información podrá dictar circulares que deberán ser publicadas en el Boletín Oficial del Estado, en las cuales se expondrá de forma detallada y concreta el contenido de la información que se vaya a solicitar, especificando de manera justificada la función para cuyo desarrollo es precisa tal información y el uso que pretende hacerse de la misma.

No obstante lo señalado en el párrafo precedente, el Ministerio de Industria, Turismo y Comercio podrá en todo caso realizar requerimientos de información particularizados sin necesidad de que previamente se dicte una circular de carácter general.

La Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información podrá realizar las inspecciones que considere necesarias con el fin de confirmar la veracidad de la información que en cumplimiento de los citados requerimientos le sea aportada.

Los datos e informaciones obtenidos por la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información en el desempeño de sus funciones, que tengan carácter confidencial por tratarse de materias protegidas por el secreto comercial, industrial o estadístico, sólo podrán ser cedidos a la Administración General del Estado y a las Comunidades Autónomas en el ámbito de sus competencias. El personal de dichas Administraciones Públicas que tenga conocimiento de estos datos estará obligado a mantener el debido secreto y sigilo respecto de los mismos.

Las entidades que deben suministrar esos datos e informaciones podrán indicar, de forma justificada, qué parte de los mismos consideran de trascendencia comercial o industrial, cuya difusión podría perjudicarles, a los efectos de que sea declarada su confidencialidad respecto de cualesquiera personas o entidades que no sean la propia Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, la Administración General del Estado o las Comunidades Autónomas, previa la oportuna justificación. La Secretaría de Estado de

Telecomunicaciones y para la Sociedad de la Información decidirá, de forma motivada, sobre la información que, según la legislación vigente, esté exceptuada del secreto comercial o industrial y sobre la amparada por la confidencialidad.

2. Son infracciones de la obligación de cumplir los requerimientos de información establecida en el apartado anterior las conductas que se tipifican en los apartados siguientes.

Las infracciones establecidas en la presente disposición adicional se entenderán sin perjuicio de las responsabilidades civiles, penales o de otro orden en que puedan incurrir los titulares de las entidades que desarrollan las actividades a que se refieren.

3. Las infracciones administrativas tipificadas en los apartados siguientes se clasifican en muy graves, graves y leves.

4. Son infracciones muy graves:

a) La negativa reiterada a facilitar a la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información la información que se reclame de acuerdo con lo previsto en la presente Ley.

b) Facilitar intencionadamente a la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información datos falsos.

5. Son infracciones graves:

La negativa expresa a facilitar a la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información la información que se reclame de acuerdo con lo previsto en la presente Ley.

6. Son infracciones leves:

No facilitar a la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información los datos requeridos o retrasar injustificadamente su aportación cuando resulte exigible.

7. Por la comisión de las infracciones señaladas en los apartados anteriores, se impondrán las siguientes sanciones:

a) Por la comisión de infracciones muy graves tipificadas en el apartado 4, multa desde 25.000 euros hasta 50.000 euros.

b) Por la comisión de infracciones graves tipificadas en el apartado 5, multa desde 5.000 euros hasta 25.000 euros.

c) Por la comisión de infracciones leves tipificadas en el apartado 6, multa de hasta 5.000 euros.

En todo caso, la cuantía de la sanción que se imponga, dentro de los límites indicados, se graduará teniendo en cuenta, además de lo previsto en el artículo 131.3 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, lo siguiente:

a) La gravedad de las infracciones cometidas anteriormente por el sujeto al que se sanciona.

b) La repercusión social de las infracciones.

c) El beneficio que haya reportado al infractor el hecho objeto de la infracción.

d) El daño causado.

Las sanciones impuestas por infracciones muy graves podrán ser publicadas en el «Boletín Oficial del Estado» una vez que la resolución sancionadora tenga carácter firme.

8. La competencia para la imposición de las sanciones muy graves corresponderá al Ministro de Industria, Turismo y Comercio y la imposición de sanciones graves y leves al Secretario de Estado de Telecomunicaciones y para la Sociedad de la Información.

El ejercicio de la potestad sancionadora se sujetará al procedimiento aplicable, con carácter general, a la actuación de las Administraciones Públicas.

9. Las estadísticas públicas que elabore la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información relativas a personas físicas ofrecerán sus datos desagregados por sexo, considerando, si ello resultase conveniente, otras variables relacionadas con el sexo para facilitar la evaluación del impacto de género y la mejora en la efectividad del principio de igualdad entre mujeres y hombres.

10. En caso de que la información recabada en ejercicio de las funciones establecidas en esta disposición adicional contuviera datos de carácter personal será de aplicación lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal y en su normativa de desarrollo.

Disposición adicional quinta. *Canalizaciones para el despliegue de redes de comunicaciones electrónicas en carreteras e infraestructuras ferroviarias de competencia estatal.*

1. Los proyectos de obras de construcción de nuevas carreteras o de nuevas líneas de ferrocarril que vayan a formar parte de las redes de interés general deberán prever, de acuerdo con lo que se determine reglamentariamente, la instalación de canalizaciones que permitan el despliegue a lo largo de las mismas de redes de comunicaciones electrónicas. Dichas canalizaciones deberán ponerse a disposición de los operadores de redes y servicios de comunicaciones electrónicas interesados en condiciones equitativas, no discriminatorias, neutrales y orientadas a costes.

Las condiciones de acceso se negociarán de mutuo acuerdo entre las partes. A falta de acuerdo, estas condiciones se establecerán mediante resolución de la Comisión del Mercado de las Telecomunicaciones.

En las mismas condiciones deberá preverse igualmente la facilitación de instalaciones para asegurar la cobertura de comunicaciones móviles en todo el recorrido, incluyendo los terrenos para la instalación de estaciones base, espacios para la instalación de los repetidores o dispositivos radiantes necesarios para garantizar la cobertura en túneles y el acceso a fuentes de energía eléctrica.

2. Sin perjuicio de la notificación a la que se refiere el artículo 6 de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, los organismos públicos responsables de la administración de las carreteras y líneas de ferrocarril de competencia estatal y las sociedades estatales que tengan encomendada su explotación podrán explotar las canalizaciones o establecer y explotar las redes de telecomunicaciones que discurran por las citadas infraestructuras de transporte en los términos previstos en la citada Ley General de Telecomunicaciones, garantizando el acceso de los restantes operadores públicos y privados a las mismas en condiciones de igualdad y neutralidad.

3. Los Ministros de Fomento y de Industria, Turismo y Comercio desarrollarán conjuntamente, en un plazo no superior a seis meses, lo establecido en esta disposición y determinarán los supuestos en que, en función del itinerario, la dimensión y demás circunstancias específicas de las nuevas carreteras o de las nuevas líneas de ferrocarril, los proyectos de obras de construcción deberán prever las canalizaciones o instalaciones a que se refiere el apartado primero.

Disposición adicional sexta. *Base de datos sobre servicios de la sociedad de la información y servicios de comunicaciones electrónicas en España.*

Con el fin de mejorar el diseño, ejecución y seguimiento de políticas relativas a la sociedad de la información, el Ministerio de Industria, Turismo y Comercio elaborará, en colaboración con las Comunidades Autónomas, una base de datos actualizada sobre los servicios de la sociedad de la información y servicios de comunicaciones electrónicas en España. Esta base de datos será sectorizada como mínimo por ámbitos territoriales de Comunidad Autónoma y los datos serán compartidos con las Administraciones que lo soliciten.

A los efectos de lo dispuesto en el párrafo anterior, el Ministerio de Industria, Turismo y Comercio podrá realizar los requerimientos de información generales o particularizados que sean necesarios en los términos previstos en la disposición adicional quinta de esta Ley.

El contenido y alcance de la base de datos referida en el párrafo primero de esta disposición adicional serán regulados mediante Orden del Ministro de Industria, Turismo y Comercio.

En lo que respecta a servicios de la sociedad de la información relativos a administración electrónica corresponderá al Ministerio de Administraciones Públicas, en colaboración con el Ministerio de Industria, Turismo y Comercio y con las Comunidades Autónomas, la regulación, elaboración y mantenimiento del correspondiente catálogo.

Disposición adicional séptima. *Agencia Estatal de Radiocomunicaciones.*

Se da nueva redacción al apartado 13 del artículo 47 de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, que queda redactado de la siguiente forma:

«La constitución efectiva de la Agencia tendrá lugar en el momento y con los plazos que señale el Real Decreto de aprobación de su Estatuto. En el citado real decreto se determinarán los órganos y servicios en que se estructurará la Agencia.»

Disposición adicional octava. *Sede de la Comisión del Mercado de las Telecomunicaciones.*

Se modifica el apartado 13 del artículo 48 de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, que queda redactado en los siguientes términos:

«13. La Comisión tendrá su sede en Barcelona y dispondrá de su propio patrimonio, independiente del patrimonio del Estado.»

Disposición adicional novena. *Modificación de la Ley 2/1995, de 23 de marzo, de Sociedades de Responsabilidad Limitada.*

Se introduce una nueva disposición final, con la siguiente redacción:

«Disposición final tercera. *Bolsa de denominaciones sociales, estatutos orientativos y plazo reducido de inscripción.*

1. Se autoriza al Gobierno para regular una Bolsa de Denominaciones Sociales con reserva.

2. Por Orden del Ministro de Justicia podrá aprobarse un modelo orientativo de estatutos para la sociedad de responsabilidad limitada.

3. Si la escritura de constitución de una sociedad de responsabilidad limitada contuviese íntegramente los estatutos orientativos a que hace referencia el apartado anterior, y no se efectuaran aportaciones no dinerarias, el registrador mercantil deberá inscribirla en el plazo máximo de cuarenta y ocho horas, salvo que no hubiera satisfecho el Impuesto de Transmisiones Patrimoniales y Actos Jurídicos Documentados en los términos previstos en la normativa reguladora del mismo.»

Disposición adicional décima. *Modificación del texto refundido de la Ley de Sociedades Anónimas, aprobado por el Real Decreto Legislativo 1564/1989, de 22 de diciembre.*

Se modifica el apartado segundo del artículo 15 del texto refundido de la Ley de Sociedades Anónimas, aprobado por el Real Decreto Legislativo 1564/1989, de 22 de diciembre, con el texto siguiente:

«No obstante, si la fecha de comienzo de las operaciones sociales coincide con la de otorgamiento de la escritura fundacional, y salvo que los estatutos sociales o la escritura dispongan otra cosa, se entenderá que los administradores ya quedan facultados para el pleno desarrollo del objeto social y para realizar toda clase de actos y contratos, de los que responderán la sociedad en formación y los socios en los términos que se han indicado.»

Disposición adicional undécima. *Acceso de las personas con discapacidad a las tecnologías de la Sociedad de la Información.*

Las Administraciones Públicas, en el ámbito de sus respectivas competencias, promoverán el impulso, el desarrollo y la aplicación de los estándares de accesibilidad para personas con discapacidad y diseño para todos, en todos los elementos y procesos basados en las nuevas tecnologías de la Sociedad de la Información.

Disposición adicional duodécima. *Lenguas Oficiales.*

Las Administraciones Públicas deberán fomentar el pluralismo lingüístico en la utilización de las nuevas tecnologías de la Sociedad de la Información, en particular en los ámbitos territoriales en que existan lenguas propias.

Disposición adicional decimotercera. *Regulación de los instrumentos telemáticos utilizados por los profesionales que elaboren proyectos e informes incorporados a procedimientos tramitados por las Administraciones.*

Las Administraciones Públicas regularán los instrumentos telemáticos necesarios para ser utilizados por los profesionales debidamente colegiados que elaboren y preparen proyectos e informes que deben incorporarse preceptivamente en los procedimientos que tramiten los órganos administrativos.

Disposición adicional decimocuarta. *Transferencia tecnológica a la sociedad.*

El Centro Nacional de Referencia de Aplicación de las Tecnologías de Información y Comunicación (CENATIC), en colaboración con los centros autonómicos de referencia y con el Centro de Transferencia de Tecnología entre Administraciones Públicas de la Administración General del Estado, se encargara de la puesta en valor y difusión entre entidades privadas y la ciudadanía en general, de todas aquellas aplicaciones que sean declaradas de fuen-

tes abiertas por las administraciones públicas, haciendo llegar a los autores o comunidades de desarrollo cualquier mejora o aportación que sea realizada sobre las mismas.

Asimismo, el CENATIC se encargará del asesoramiento general sobre los aspectos jurídicos, tecnológicos y metodológicos más adecuados para la liberación del software y conocimiento.

Disposición adicional decimoquinta. *Fomento a la participación ciudadana en la sociedad de la información.*

Con el objeto de fomentar la presencia de la ciudadanía y de las entidades privadas sin ánimo de lucro y garantizar el pluralismo, la libertad de expresión y la participación ciudadana en la sociedad de la información, se establecerán medios de apoyo y líneas de financiación para el desarrollo de servicios de la sociedad de la información sin finalidad lucrativa que, promovidos por entidades ciudadanas, fomenten los valores democráticos y la participación ciudadana, atiendan al interés general o presten servicio a comunidades y grupos sociales desfavorecidos.

Disposición adicional decimosexta. *Contenidos digitales de titularidad pública para su puesta a disposición de la sociedad.*

Siempre que por su naturaleza no perjudique al normal funcionamiento de la Administración, ni afecte al interés público o al interés general, los contenidos digitales o digitalizados de que dispongan las Administraciones Públicas, cuyos derechos de propiedad intelectual le pertenezcan sin restricciones o sean de dominio público, serán puestos a disposición del público, en los términos legalmente establecidos, de forma telemática sin restricciones tecnológicas, para su uso consistente en el estudio, copia o redistribución, siempre que las obras utilizadas de acuerdo con lo anteriormente señalado citen al autor y se distribuyan en los mismos términos.

Disposición adicional decimoséptima. *Cesión de contenidos para su puesta a disposición de la sociedad.*

Las personas físicas o jurídicas podrán ceder sus derechos de explotación sobre obras para que una copia digitalizada de las mismas pueda ser puesta a disposición del público de forma telemática, sin restricciones tecnológicas o metodológicas, y libres para ser usado con cualquier propósito, estudiados, copiados, modificados y redistribuidos, siempre que las obras derivadas se distribuyan en los mismos términos.

Disposición adicional decimoctava. *Televisión de proximidad sin ánimo de lucro.*

1. El Ministerio de Industria, Turismo y Comercio, a través de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, mediante Resolución del Secretario de Estado, planificará frecuencias para la gestión indirecta del servicio de televisión local de proximidad por parte de entidades sin ánimo de lucro que se encontraran habilitadas para emitir al amparo de la Disposición Transitoria Primera de la Ley 41/1995, de 22 de diciembre, de Televisión Local por Ondas Terrestres, siempre que se disponga de frecuencias para ello.

Tienen la consideración de servicios de difusión de televisión de proximidad aquellos sin finalidad comercial que, utilizando las frecuencias que en razón de su uso por servicios próximos no estén disponibles para servicios de difusión de televisión comercialmente viables, están dirigidos a comunidades en razón de un interés cultural, educativo, étnico o social.

El canal de televisión difundido lo será siempre en abierto. Su programación consistirá en contenidos originales vinculados con la zona y comunidad a la que vayan dirigidos y no podrá incluir publicidad ni televenta, si bien se admitirá el patrocinio de sus programas.

La entidad responsable del servicio de televisión local de proximidad no podrá ser titular directa o indirectamente de ninguna concesión de televisión de cualquier cobertura otorgada por la Administración que corresponda.

2. Corresponde al Gobierno aprobar el reglamento general de prestación del servicio, con carácter de norma básica, y el reglamento técnico, en el que se establezca el procedimiento para la planificación de las frecuencias destinadas a servicios de difusión de televisión de proximidad, atendiendo entre otros extremos a las necesidades de cobertura, población y características propias de este servicio.

Dicho reglamento establecerá las condiciones técnicas que deberán reunir las frecuencias destinadas a estos servicios, la extensión máxima de la zona de servicio, la determinación concreta de las potencias de emisión, características y uso compartido del múltiplex asignado para la prestación del servicio y el procedimiento por el que las Comunidades Autónomas solicitarán la reserva de frecuencias para estos servicios, así como el procedimiento de asignación por parte de la Agencia Estatal de Radiocomunicaciones.

La planificación del espectro para la televisión de proximidad no será prioritaria con respecto a otros servicios planificados o planificables.

3. Será de aplicación a estas televisiones lo dispuesto en la Ley 25/1994, de 12 de julio, por la que se incorpora al ordenamiento jurídico español la Directiva 89/552/CEE, sobre la coordinación de disposiciones legales, reglamentarias y administrativas de los Estados miembros, relativas al ejercicio de actividades de radiodifusión televisiva, y lo previsto en los artículos 1, 2, 6, apartados 2 y 3 del artículo 9, 10, 11, 15, 18, 20, 21, 22 y apartado 4 de la disposición transitoria segunda de la Ley 41/1995, de 22 de diciembre, de Televisión Local por Ondas Terrestres. Igualmente les será de aplicación lo dispuesto en la Disposición Adicional Trigésima de la Ley 62/2003, de 30 de diciembre, de Medidas fiscales, administrativas y del orden social.

4. Las Comunidades Autónomas adjudicarán las correspondientes concesiones para la prestación de servicios de televisión de proximidad, de acuerdo con el reglamento general de prestación del servicio y su normativa.

5. Las concesiones para la prestación de servicios de difusión de radio y televisión de proximidad se otorgarán por un plazo de cinco años y podrán ser renovadas hasta en tres ocasiones, siempre que su actividad no perjudique la recepción de los servicios de difusión legalmente habilitados que coincidan total o parcialmente con su zona de cobertura.

Estas concesiones obligan a la explotación directa del servicio y serán intransferibles.

6. Las concesiones para la prestación de servicios de televisión de proximidad se extinguirán, además de por alguna de las causas generales previstas en el artículo 15 de la Ley 41/1995, de 22 de diciembre, de Televisión Local por Ondas Terrestres, por extinción de la personalidad jurídica de su titular y por su revocación.

7. Serán causas de revocación de la concesión la utilización de las mismas para la difusión de servicios comerciales y la modificación de las condiciones de planificación del espectro radioeléctrico sin que exista una frecuencia alternativa.

Disposición adicional decimonovena. *Modificación de la Ley 22/2007, de 11 de julio, sobre comercialización a distancia de servicios financieros destinados a los consumidores y de la Ley 36/2007, de 16 de noviembre, por la que se modifica la Ley 13/1985, de 25 de mayo, de coeficientes de inversión, recursos propios y obligaciones de información de los intermediarios financieros y otras normas del sistema financiero.*

1. Se modifica la letra b) de la Disposición Derogatoria de la Ley 22/2007, de 11 de julio, sobre comercialización a distancia de servicios financieros destinados a los consumidores, que tendrá la siguiente redacción:

«b) El párrafo segundo del apartado 1 del artículo 83.a) de la Ley 50/1980, de 8 de octubre, de Contrato de Seguro.»

2. Se modifican los apartados 2, 3 y 4 de la Disposición transitoria primera de la Ley 36/2007, de 16 de noviembre, por la que se modifica la Ley 13/1985, de 25 de mayo, de coeficientes de inversión, recursos propios y obligaciones de información de los intermediarios financieros y otras normas del sistema financiero, que tendrán la siguiente redacción:

«2. Durante el primer y segundo período de doce meses posteriores al 31 de diciembre de 2007, las entidades de crédito o los grupos consolidables de entidades de crédito que utilicen los métodos internos de medición de riesgo operacional mantendrán recursos propios que serán en todo momento iguales o superiores a los importes indicados en los apartados 3 y 4.

3. Para el primer período de doce meses previsto en el apartado 1 y en el apartado 2, el importe de los recursos propios será el 90 por ciento del importe total de los recursos propios mínimos que serían exigibles a la entidad o grupo de mantenerse la regulación vigente a 31 de diciembre de 2007.

4. Para el segundo período de doce meses contemplado en el apartado 1 y en el apartado 2, el importe de los recursos propios será el 80 por ciento del importe total de los recursos propios mínimos que serían exigibles a la entidad o grupo de mantenerse la regulación vigente a 31 de diciembre de 2007.»

Disposición adicional vigésima. *Regulación del juego.*

El Gobierno presentará un Proyecto de Ley para regular las actividades de juego y apuestas, en particular las realizadas a través de sistemas interactivos basados en comunicaciones electrónicas, que atenderá a los siguientes principios:

1. Asegurar la compatibilidad de la nueva regulación con la normativa aplicable a otros ámbitos vinculados a la prestación de este tipo de servicios, y, en especial, a la normativa de protección de los menores, de la juventud, de grupos especialmente sensibles de usuarios así como de los consumidores en general, además del ámbito de protección de datos de carácter personal y de servicios de la Sociedad de la Información.

2. Establecer una regulación sobre la explotación de actividades de juego por sistemas interactivos de acuerdo con la normativa y los principios generales del derecho comunitario.

3. Articular un sistema de control sobre los servicios de juego y apuestas por sistemas interactivos que garantice unas condiciones de mercado plenamente seguras y equitativas para los operadores de tales sistemas así como unos adecuados niveles de protección de los usuarios. En particular, deberá regular la actividad de aquellos operadores que ya cuenten con una autorización para la presentación de los mencionados servicios otorgada por las autoridades de cualquiera de los Estados miembros de la Unión Europea.

4. Establecer un sistema de tributación sobre los servicios de juego y apuestas por sistemas interactivos atendiendo al origen de las operaciones objeto de tributación. La regulación deberá igualmente prever un sistema de distribución de la tributación obtenida como consecuencia de la explotación de servicios de juego y apuestas por medios electrónicos en España entre la Administración Estatal y las Comunidades Autónomas, teniendo en cuenta la especificidad fiscal de los regímenes forales.

5. La actividad de juego y apuestas a través de sistemas interactivos basados en comunicaciones electrónicas sólo podrá ejercerse por aquellos operadores autorizados para ello por la Administración Pública competente, mediante la concesión de una autorización tras el cumplimiento de las condiciones y requisitos que se establezcan. Quien no disponga de esta autorización no podrá realizar actividad alguna relacionada con los juegos y apuestas interactivos. En particular, se establecerán las medidas necesarias para impedir la realización de publicidad por cualquier medio así como la prohibición de utilizar cualquier medio de pago existente en España. Por otra parte, se sancionará de conformidad con la legislación de represión del contrabando la realización de actividades de juego y apuestas a través de sistemas interactivos sin contar con la autorización pertinente.

6. La competencia para la ordenación de las actividades de juegos y apuestas realizadas a través de sistemas interactivos corresponderá a la Administración General del Estado cuando su ámbito sea el conjunto del territorio nacional o abarque más de una Comunidad Autónoma.

Disposición transitoria única. *Régimen transitorio relativo a las tarifas aplicables por la asignación, renovación y otras operaciones registrales de los nombres de dominio bajo el «.es».*

Hasta que se fijen, de conformidad con lo que se establece en el artículo 8 de esta Ley, los precios públicos aplicables por la asignación, renovación y otras operaciones registrales de los nombres de dominio bajo el «.es» seguirán siendo de aplicación las tasas correspondientes fijadas de acuerdo con las normas legales y disposiciones reglamentarias de desarrollo vigentes con anterioridad a la entrada en vigor de esta Ley.

Disposición final primera. *Fundamento constitucional.*

1. Tienen el carácter de legislación básica los siguientes preceptos de esta Ley:

a) Los apartados 2, 3 y 5 del artículo 1 y los artículos 2 y 6, que se dictan al amparo de lo dispuesto en el apartado 13.º del artículo 149.1 de la Constitución.

b) Los apartados 1 y 4 del artículo 1, la disposición adicional duodécima y la disposición adicional decimotercera, que se dictan al amparo de lo dispuesto en el artículo 149.1.18.ª de la Constitución.

c) La disposición adicional undécima, que se dicta al amparo de lo dispuesto en el artículo 149.1.1.ª y 18.ª de la Constitución.

d) La disposición adicional decimoquinta, que se dicta al amparo de lo dispuesto en el artículo 149.1.1.ª de la Constitución.

2. Los artículos 3, 4 y 5 de esta Ley se dictan al amparo de lo dispuesto en el artículo 149.1. 6.ª, 8.ª y 21.ª de la Constitución, sin perjuicio de las competencias que ostenten las Comunidades Autónomas.

3. Los artículos 7 y 8 y las disposiciones adicionales primera, segunda, tercera, cuarta, quinta, sexta, séptima, octava y decimocuarta de esta Ley se dictan al amparo de lo dispuesto en el artículo 149.1.21.ª de la Constitución.

4. Las disposiciones adicionales novena y décima de esta Ley se dictan al amparo de lo dispuesto en el artículo 149.1.6.ª y 8.ª de la Constitución.

5. Las disposiciones adicionales decimosexta y decimoséptima de esta Ley se dictan al amparo de lo dispuesto en el artículo 149.1.9.ª de la Constitución.

Disposición final segunda. *Modificación de leyes por las que se incorpora derecho comunitario.*

Mediante esta Ley se modifica la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico y la Ley 59/2003, de 19 de diciembre, de Firma Electrónica que incorporaron respectivamente la Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior, y la Directiva 1999/93/CE, del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica.

Disposición final tercera. *Habilitación al Gobierno.*

Se habilita al Gobierno para desarrollar mediante Reglamento lo previsto en esta Ley, en el ámbito de sus competencias.

Disposición final cuarta. *Entrada en vigor.*

Esta Ley entrará en vigor al día siguiente de su publicación en el Boletín Oficial del Estado.

No obstante, las obligaciones contenidas en el nuevo artículo 12 bis de la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico entrarán en vigor a los tres meses de la publicación de la Ley en el Boletín Oficial del Estado, y los artículos 2 y 6 de esta Ley entrarán en vigor a los doce meses de la publicación de la Ley en el Boletín Oficial del Estado.

Por tanto,

Mando a todos los españoles, particulares y autoridades que guarden y hagan guardar esta ley.

Madrid, 28 de diciembre de 2007.

JUAN CARLOS R.

El Presidente del Gobierno,
JOSÉ LUIS RODRÍGUEZ ZAPATERO

MINISTERIO DE ECONOMÍA Y HACIENDA

22441 *CORRECCIÓN de errores del Real Decreto 1514/2007, de 16 de noviembre, por el que se aprueba el Plan General de Contabilidad.*

Advertidos errores en el suplemento del Real Decreto 1514/2007, de 16 de noviembre, por el que se aprueba el Plan General de Contabilidad, publicado en el «Boletín Oficial de Estado» número 278, de 20 de noviembre de 2007, se transcriben a continuación las oportunas rectificaciones:

En la página 25, segunda columna, en el apartado 2.5.3, párrafo segundo, en las líneas 18 y 19, debe eliminarse la frase: «… que correspondan a elementos identificables en el balance de la participada.»

En la página 40, segunda columna, en la letra c) del apartado 2.7, donde dice: «... de la empresa neto del efecto impositivo», debe decir: «... de la empresa neta del efecto impositivo».

En la página 28, segunda columna, en el apartado 3.2, en la última línea del sexto párrafo, donde dice: «mimo», debe decir: «mismo».

Los cuadros que figuran en las páginas 49, 50 y 51, deben ser sustituidos por los siguientes[1]:

[1] Figuran en anexo I.