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