Glosario de términos de ciberseguridad

Una guía de aproximación para el empresario

Glosario de términos de ciberseguridad

Una guía de aproximación para el empresario

Índice

1. Introducción

Este glosario recoge los términos de seguridad que han ido apareciendo en las entradas en el blog de empresas **de Netebu**

Para la definición de los términos se han utilizado las fuentes de referencia, la Wikipedia o el propio portal de **Netebu** u otros documentos propios, como guías e informes. Para todos ellos se ha primado que el lenguaje sea adecuado al público objetivo ante la precisión técnica.

El glosario está ordenado alfabéticamente. Cada entrada contiene una definición salvo que se haya preferido otro término, como más común, en cuyo caso aparece la referencia al término definido introducida por: "Véase:" También se han incluido sinónimos o términos relacionados en las entradas con definición si los hubiera.

2. Definiciones

2.1. A

2.1.1. Activo de información

Definición:
Es cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización, pueden ser procesos de negocio, datos, aplicaciones, equipos informáticos, personal, soportes de información, redes, equipamiento auxiliar o instalaciones. Es susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización.

2.1.2. Acuerdo de licencia

Definición:
Es una cesión de derechos entre un titular de derechos de propiedad intelectual (licenciante) y otra persona que recibe la autorización de utilizar dichos derechos (licenciatario) a cambio de un pago convenido de antemano (tasa o regalía) o de unas condiciones determinadas. Existen distintos tipos de acuerdos de licencias que pueden clasificarse en las siguientes categorías:

- acuerdos de licencia tecnológica
- acuerdos de licencia y acuerdos de franquicia sobre marcas
- acuerdos de licencia sobre derecho de autor

2.1.3. Administración Electrónica

Definición:
Actividad consistente en la prestación de servicios a ciudadanos y empresas mediante la utilización de medios telemáticos y definida en la Ley 11/2007 de 22 de junio de acceso electrónico de los ciudadanos a los servicios públicos. Esta actividad compete a las Administraciones Públicas con el objeto de simplificar los procedimientos con la Administración, manteniendo al mismo tiempo, los niveles adecuados de seguridad jurídica y procurando la mejora de calidad de los servicios.

Entre las principales finalidades que persigue la Administración Electrónica se encuentran:

- el impulso en la utilización de las nuevas tecnologías de la información y las comunicaciones
- la búsqueda de transparencia y confianza por parte de ciudadanos y empresas
- la simplificación en los procedimientos y trámites administrativos
- el impulso en el crecimiento y desarrollo de la Sociedad de la Información

Sinónimo: e-Administración.

2.1.4. Adware

Definición:
Es cualquier programa que automáticamente va mostrando publicidad al usuario durante su instalación o durante su uso y con ello genera beneficios a sus creadores.

Aunque se asocia al *malware,* no tiene que serlo forzosamente, ya que puede ser un medio legítimo usado por desarrolladores de *software* que lo implementan en sus programas, generalmente en las versiones *shareware*, haciéndolo desaparecer en el momento en que adquirimos la versión completa del programa. Se convierte en *malware* en el momento en que empieza a recopilar información sobre el ordenador donde se encuentra instalado.

Sinónimo: *Malvertising*

2.1.5. Agujero de seguridad

Definición:
Véase: Vulnerabilidad

2.1.6. Algoritmos de cifrado

Definición:
Operación o función matemática utilizada en combinación con una clave que se aplica a un texto en claro y permite obtener un texto cifrado (o descifrarlo) garantizando la confidencialidad e integridad de la información contenida. Existen dos tipos de cifrado atendiendo a las características de las claves de cifrado, estos son el cifrado simétrico y cifrado asimétrico.

- El cifrado simétrico, también conocido como cifrado de clave secreta, es la técnica más antigua y en ella se utiliza la misma clave para cifrar y descifrar la información.
- El cifrado asimétrico, o cifrado de clave pública, es una técnica de codificación que utiliza un par de claves diferentes para el cifrado y descifrado de información y garantiza el no repudio, aparte de la confidencialidad y la integridad.

Sinónimo: *Cifrado*

2.1.7. Amenaza

Definición:
Circunstancia desfavorable que puede ocurrir y que cuando sucede tiene consecuencias negativas sobre los activos provocando su indisponibilidad, funcionamiento incorrecto o pérdida de valor. Una amenaza puede tener causas naturales, ser accidental o intencionada. Si esta circunstancia desfavorable acontece a la vez que existe una vulnerabilidad o debilidad de los sistemas o aprovechando su existencia, puede derivar en un incidente de seguridad.

2.1.8. Antivirus

Definición:
Es un programa informático específicamente diseñado para detectar, bloquear y eliminar código malicioso (virus, troyanos, gusanos, etc.), así como proteger los equipos de otros programas peligrosos conocidos genéricamente como *malware*.

La forma de actuar del antivirus parte de una base de datos que contiene parte de los códigos utilizados en la creación de virus conocidos. El programa antivirus compara el código binario de cada archivo ejecutable con esta base de datos. Además de esta técnica, se valen también de procesos de monitorización de los programas para detectar si éstos se comportan como programas maliciosos.

«El análisis de riesgos comprende la identificación de activos de información, sus vulnerabilidades y las amenazas»

Es importante hacer notar que para un correcto funcionamiento del antivirus, éste debe estar activado y actualizado en todo momento.

Sinónimo: *Antimalware*

2.1.9. Análisis de riesgos

Definición:
Es un proceso que comprende la identificación de activos de información, sus vulnerabilidades y las amenazas a los que se encuentran expuestos, así como la probabilidad de ocurrencia y el impacto de las mismas, a fin de determinar los controles adecuados para tratar el riesgo.

2.1.10. Ataque diccionario

Definición:
Véase: Ataque de fuerza bruta

2.1.11. Ataque de fuerza bruta

Definición:
Un ataque de fuerza bruta es un procedimiento para averiguar una contraseña que consiste en probar todas las combinaciones posibles hasta encontrar la combinación correcta.

Los ataques por fuerza bruta, dado que utilizan el método de prueba y error, tardan mucho tiempo en encontrar la combinación correcta (hablamos en ocasiones de miles años), por esta razón, la fuerza bruta suele combinarse con un ataque de diccionario.

2.1.12. Ataque combinado

Definición:
Es uno de los ataques más agresivos ya que se vale de métodos y técnicas muy sofisticadas que combinan distintos virus informáticos, gusanos, troyanos y códigos maliciosos, entre otros.

Esta amenaza se caracteriza por utilizar el servidor y vulnerabilidades de Internet para iniciar, transmitir y difundir el ataque extendiéndose rápidamente y ocasionando graves daños, en su mayor parte, sin requerir intervención humana para su propagación.

Las principales características que presenta este ataque son:

- Los daños producidos van desde ataques de denegación de servicio (DoS), pasando por ataques en la dirección IP o daños en un sistema local; entre otros.
- Tiene múltiples métodos de propagación.

- El ataque puede ser múltiple, es decir, puede modificar varios archivos y causar daños en varias áreas a la vez, dentro de la misma red.
- Toma ventaja de vulnerabilidades ya conocidas en ordenadores, redes y otros equipos.
- Obtiene las contraseñas por defecto para tener accesos no autorizados.
- Se propaga sin intervención humana.

2.1.13. Ataque de repetición

Definición:
Es un tipo de ataque en el cual el atacante captura la información que viaja por la red, por ejemplo un comando de autenticación que se envía a un sistema informático, para, posteriormente, enviarla de nuevo a su destinatario, sin que este note que ha sido capturada. Si el sistema informático o aplicación es vulnerable a este tipo de ataques, el sistema ejecutará el comando, como si fuera legítimo, enviando la respuesta al atacante que puede así obtener acceso al sistema.

Para protegerse de este tipo de ataques el sistema informático puede tomar medidas como usar un control de identificación de comandos, de sellado de tiempos (*timestamp*), etc. junto con el cifrado y la firma de los comandos con el fin de evitar que sean reutilizados.

2.1.14. Auditoría de seguridad

Definición:
Es el estudio que comprende el análisis y gestión de sistemas llevado a cabo por profesionales en tecnologías de la información (TI) con el objetivo de identificar, enumerar y describir las diversas vulnerabilidades que pudieran presentarse en una revisión exhaustiva de las estaciones de trabajo, redes de comunicaciones, servidores o aplicaciones.

2.1.15. Autenticación

Definición:
Procedimiento para comprobar que alguien es quién dice ser cuando accede a un ordenador o a un servicio online. Este proceso constituye una funcionalidad característica para una comunicación segura.

2.1.16. Autenticidad

Definición:
Véase: No repudio

2.1.17. Autoridad de certificación

Definición
La Autoridad de Certificación (AC o CA, por sus siglas en inglés, *Certification Authority*) es una entidad de confianza cuyo objeto es garantizar la identidad de los titulares de certificados digitales y su correcta asociación a las claves de firma electrónica.

2.1.18. Autoridad de registro

Definición:
Es la entidad encargada de identificar de manera inequívoca a los usuarios para que, poste-

riormente, éstos puedan obtener certificados digitales.

Sinónimo: Autoridad Local de Registro

2.1.19. Autoridad de validación

Definición:
Entidad que informa de la vigencia y validez de los certificados electrónicos creados y registrados por una Autoridad de Registro y por una Autoridad de Certificación. Asimismo, las autoridades de validación almacenan la información sobre los certificados electrónicos anulados en las listas de revocación de certificados (CRL).
Resumiendo el proceso, cuando un cliente consulta el estado en que se encuentra un certificado electrónico a una autoridad de validación, ésta comprueba en su CRL el estado del mismo, contestando mediante el protocolo de transferencia de hipertexto HTTP.

Actualmente, en España son autoridades de validación:

- La Fábrica Nacional de Moneda y Timbre presta sus servicios de validación con carácter universal: ciudadanos, empresas y Administraciones Públicas.
- La plataforma @firma del Ministerio de Administraciones Públicas presta los servicios de validación al conjunto de las Administraciones Públicas.

2.1.20. Aviso Legal

Definición:
Un aviso legal es un documento, en una página web, donde se recogen las cuestiones legales que son exigidas por la normativa de aplicación. El aviso legal puede incluir:

1. Términos y condiciones de uso
2. Política de privacidad y protección de datos si recogen datos de carácter personal según la LOPD (formularios, registro de usuarios,…)
3. Información general a la que se hace referencia en al artículo 10 de la LSSI-CE y otra información relativa al uso de *cookies*, contratación, etc. si aplicara.
4. Qué elementos están sujetos a los derechos de propiedad intelectual e industrial, entre otros:

   - la propia información de la web
   - el diseño gráfico
   - las imágenes
   - el código fuente
   - las marcas
   - los nombres comerciales
   - el diseño del sitio web

2.2. B

2.2.1. B2B

Definición:
Abreviatura de «*Business to Business*». Este término se refiere a las transacciones comerciales entre empresas, utilizando medios telemáticos como *EDI* (*Electronic Data Interchange*) o

el Comercio Electrónico.

Algunas de las ventajas que aporta el *business-to-business* para las empresas implicadas son:

- Rapidez y seguridad de las comunicaciones.
- Integración directa de los datos de la transacción en los sistemas informáticos de la empresa.
- Posibilidad de recibir mayor número de ofertas o demandas, ampliando la competencia.
- Despersonalización de la compra con lo que se evitan posibles tratos de favor.
- Abaratamiento del proceso: menos visitas comerciales, proceso de negociación más rápido, etc. Por tanto, los compradores pueden pedir una reducción de precios en virtud del menor coste de gestión, o los vendedores incrementar su margen comercial.

2.2.2. B2C

Definición:
Abreviatura de *«Business to Consumer».* Este término se refiere a la estrategia que desarrollan las empresas comerciales para llegar directamente al cliente o consumidor final.

Suele también indicar las transacciones realizadas directamente entre un cliente y una empresa sin que medie un intermediario.

2.2.3. Backdoor

Definición:
Véase: Puerta trasera

2.2.4. Backup

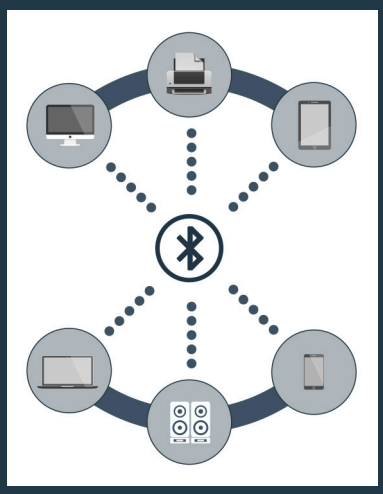
Definición:
Copia de seguridad que se realiza sobre ficheros o aplicaciones contenidas en un ordenador con la finalidad de recuperar los datos en el caso de que el sistema de información sufra daños o pérdidas accidentales de los datos almacenados.

Los dispositivos más empleados para llevar a cabo la técnica de *backup* pueden ser discos duros, discos ópticos, USB o DVD. También es común la realización de copias de seguridad mediante servicios de copia basados en la nube. Es de suma importancia mantener actualizada la copia de seguridad así como tener la máxima diligencia de su resguardo, para evitar pérdidas de información que pueden llegar a ser vitales para el funcionamiento ya sea de una empresa, institución o de un contenido de tipo personal. Además, cada cierto tiempo es conveniente comprobar que la copia de seguridad puede restaurarse con garantías.

Sinónimo: Copia de seguridad, copia de respaldo

2.2.5. BIA

Definición:
Abreviatura de *«Business Impact Analysis»*. Se trata de un informe que nos muestra el coste ocasionado por la interrupción de los procesos críticos de negocio. Este informe nos permitirá asignar una criticidad a los procesos de negocio, definir los objetivos de recuperación y determinar un tiempo de recuperación a cada uno de ellos.



«El objetivo del Bluetooth es eliminar los cables en las conexiones entre dispositivos electrónicos»

2.2.6. Biometría

Definición:
La biometría es un método de reconocimiento de personas basado en sus características fisiológicas (huellas dactilares, retinas, iris, cara, etc.) o de comportamiento (firma, forma de andar, tecleo, etc.). Se trata de un proceso similar al que habitualmente realiza el ser humano reconociendo e identificando a sus congéneres por su aspecto físico, su voz, su forma de andar, etc.

Para la identificación del individuo es necesario que los rasgos o características analizadas sean de carácter universal, ser lo suficientemente distintas a las de otra persona, permanecer de forma constante e invariante en el individuo y además, poder ser medida.

2.2.7. Bluetooth

Definición:
La tecnología *Bluetooth* es una tecnología inalámbrica de radio de corto alcance, cuyo objetivo es eliminar los cables en las conexiones entre dispositivos electrónicos, simplificando así las comunicaciones entre teléfonos móviles, ordenadores, cámaras digitales y otros dispositivos informáticos operando bajo la banda de radio de 2.4 GHz de frecuencia.

Este protocolo ofrece a los dispositivos la posibilidad de comunicarse cuando se encuentran a una distancia de hasta 10 metros, incluso a pesar de que pueda existir algún obstáculo físico o a pesar de que los usuarios de los dispositivos se encuentren en distintas habitaciones de un mismo emplazamiento.

Algunas aplicaciones de los dispositivos *Bluetooth* son:

- Intercambio de ficheros, fichas de contacto, recordatorios.
- Comunicación sin cables entre ordenadores y dispositivos de entrada y salida (impresoras, teclado, ratón).
- Conexión a determinados contenidos en áreas públicas.

2.2.8. Bomba Lógica

Definición:
Trozo de código insertado intencionalmente en un programa informático que permanece oculto hasta cumplirse una o más condiciones preprogramadas, momento en el que se ejecuta una acción maliciosa.

La característica general de una bomba lógica y que lo diferencia de un virus es que este código insertado se ejecuta cuando una determinada condición se produce, por ejemplo, tras encender el ordenador una serie de veces, o pasados una serie de días desde el momento en que

la bomba lógica se instaló en nuestro ordenador.

2.2.9. Botnet

Definición:
Una *botnet* es un conjunto de ordenadores (denominados *bots*) controlados remotamente por un atacante que pueden ser utilizados en conjunto para realizar actividades maliciosas como envío de *spam*, ataques de *DDoS*, etc.

Las *botnets* se caracterizan por tener un servidor central (*C&C*, de sus siglas en inglés *Command & Control*) al que se conectan los *bots* para enviar información y recibir comandos.

Existen también las llamadas *botnets P2P* que se caracterizan por carecer de un servidor *C&C* único.

2.2.10. Bug

Definición:
Es un error o fallo en un programa de dispositivo o sistema de *software* que desencadena un resultado indeseado.

Sinónimo: Error de *software*

2.2.11. Bulo

Definición:
También llamados *hoax*, son noticias falsas creadas para su reenvío masivo ya sea a través de redes sociales, mensajería instantánea o correo electrónico, con el fin de hacer creer al destinatario que algo es falso.

Pueden ser varias las motivaciones para crear este tipo de noticias, como difundir información falsa en perjuicio de terceras personas u organismos o incitar al receptor del mensaje a causar daños en su propio ordenador.

Sinónimo: *Hoax*

2.3. C

2.3.1. Cartas nigerianas

Definición:
Se trata de una comunicación inesperada mediante correo electrónico carta o mensajería instantánea en las que el remitente promete negocios muy rentables.

La expectativa de poder ganar mucho dinero mediante unas sencillas gestiones, es el gancho utilizado por los estafadores para involucrar a las potenciales víctimas en cualquier otra situación engañosa, procurando que finalmente transfiera una fuerte cantidad de dinero para llevar a cabo la operación.

El funcionamiento es muy variado, pero a grandes rasgos se podría resumir así:

Un remitente desconocido contacta con la potencial victima haciéndose pasar por un abogado, familiar o amigo cercano de un miembro del Gobierno o de un importante hombre de negocios que ha perdido la vida en un accidente o similar. Según esta comunicación, antes de morir esa persona, depositó una gran cantidad de dinero en una cuenta bancaria. El remitente asegura que tiene acceso legal a esa cuenta y pretende transferir el dinero a una cuenta en el extranjero.

El remitente ha encontrado el nombre y la dirección de la víctima por recomendación de otra persona o por casualidad y la víctima es la única persona de confianza que puede ayudarle a realizar la transferencia del dinero.

Por su asistencia, promete a la víctima, un porcentaje de la cantidad total de dinero y solicita discreción para llevar a cabo el negocio. La víctima debe abrir una cuenta en un banco determinado para que pueda remitirle el dinero y generalmente pagar por adelantado unos gastos para la transferencia del dinero.
La siguiente fase del fraude consiste en convencer a la victima de que la transferencia de dinero está en proceso. Para ello, mandan a la víctima documentos aparentemente oficiales, al igual que cartas y movimientos bancarios falsos.

Sin embargo esta transferencia del dinero por parte de los estafadores nunca llega a tener lugar.

Sinónimo: Estafa nigeriana

2.3.2. Centro de respaldo

Definición:
Un centro de respaldo es un centro de procesamiento de datos (CPD) específicamente diseñado para tomar el control de otro CPD principal en caso de contingencia.

Las características de un centro de respaldo deben ser las siguientes:

- Su localización debe ser totalmente distinta a la del CPD principal con el objeto de que no se vean ambos afectados simultáneamente por la misma contingencia. Es habitual situarlos entre 20 y 40 kilómetros del CPD principal.
- El equipamiento electrónico e informático del centro de respaldo debe ser absolutamente compatible con el existente en el CPD principal.
- El equipamiento *software* debe ser idéntico al existente en el CPD principal. Esto implica exactamente las mismas versiones y parches del software de base y de las aplicaciones corporativas que estén en explotación en el CPD principal. De otra manera, no se podría garantizar totalmente la continuidad de operación.
- Por último, es necesario contar con una réplica de los mismos datos con los que se trabaja en el CPD original.

2.3.3. Certificado de autenticidad

Definición:
El Certificado de autenticidad (COA) es una etiqueta especial de seguridad que acompaña a un *software* con licencia legal para impedir falsificaciones.

El COA suele ir pegado en el embalaje del *software*, y permite asegurar que el *software* y los

demás elementos que contenga, como los medios y los manuales, son auténticos.

En ocasiones el *software* viene preinstalado al comprar un equipo. En esos casos el COA suele encontrarse en el exterior del equipo. Si se trata de un dispositivo pequeño (con una longitud o anchura de 15 cm o menos), el COA puede encontrarse bajo la batería.

2.3.4. Certificado digital

Definición:
Un certificado digital es un fichero informático generado por una entidad denominada Autoridad Certificadora (CA) que asocia unos datos de identidad a una persona física, organismo o empresa confirmando de esta manera su identidad digital en Internet.

El certificado digital es válido para autenticar la existencia y validez de un usuario o sitio web por lo que es necesaria la colaboración de un tercero que sea de confianza para cualquiera de las partes que participe en la comunicación. El nombre asociado a esta entidad de confianza es Autoridad Certificadora pudiendo ser un organismo público o empresa reconocida en Internet. El certificado digital tiene como función principal autenticar al poseedor pero puede servir también para cifrar las comunicaciones y firmar digitalmente. En algunas administraciones públicas y empresas privadas es requerido para poder realizar ciertos trámites que involucren intercambio de información sensible entre las partes.

2.3.5. Cesión de datos

Definición:
La cesión de datos es la comunicación de datos de carácter personal a una tercera persona sin el consentimiento del interesado.

La comunicación de este tipo de datos está regulada en el artículo 11 de la LOPD, mientras que la comunicación de datos entre Administraciones públicas se regula en el artículo 21 de dicha ley.

2.3.6. Cifrado

Definición:
Véase: Algoritmos de cifrado

2.3.7. Clave pública

Definición:
Los sistemas de criptografía asimétrica, se basan en la generación, mediante una «infraestructura de clave pública», de un par de claves, denominadas clave pública y clave privada, que tienen la peculiaridad de que los mensajes cifrados con una de ellas sólo pueden ser descifrados utilizando la otra.

Así, se conoce como clave pública a una de estas claves, que puede ponerse en conocimiento de todo el mundo y que utilizará un remitente para cifrar el mensaje o documento que quiere enviar, garantizando de esta forma que tan solo pueda descifrarlo el destinatario con su clave privada.

2.3.8. Clave privada

«El control parental evita que los menores de edad hagan un uso indebido del ordenador»

Definición:
Los sistemas de criptografía asimétrica, se basan en la generación de un par de claves, denominadas clave pública y clave privada, que tienen la peculiaridad de que los mensajes cifrados con una de ellas sólo pueden ser descifrados utilizando la otra.

En este tipo de sistemas, la clave privada sólo debe ser conocida por el usuario para el cifrado y descifrado de mensajes.

El hecho de que la clave privada sólo sea conocida por su propietario persigue dos objetivos:

- Cualquier documento generado a partir de esta clave necesariamente tiene que haber sido generado por el propietario de la clave (firma electrónica).
- Un documento al que se aplica la clave pública sólo podrá ser abierto por el propietario de la correspondiente clave privada (cifrado electrónico).

Estos sistemas de criptografía constituyen un elemento esencial para la propia seguridad del tráfico jurídico y el desarrollo de transacciones económicas o el comercio on-line.

2.3.9. Cloud computing

Definición:
El término *cloud computing* o computación en la nube se refiere a un paradigma que permite ofrecer servicios de computación a través de una red, que usualmente es Internet.
Esta tendencia permite a los usuarios almacenar información, ficheros y datos en servidores de terceros, de forma que puedan ser accesibles desde cualquier terminal con acceso a la nube o a la red, resultando de esta manera innecesaria la instalación de *software* adicional (al que facilita el acceso a la red) en el equipo local del usuario.

Importantes plataformas ofrecen herramientas y funcionalidades de este tipo y aunque conlleva una importante dinamización y libertad, se debe prestar especial atención a la seguridad de la información, particularmente desde el punto de vista de la protección de la intimidad y de los datos personales, ya que la información, documentos y datos se encuentran almacenados en servidores de terceros sobre los que generalmente no se tiene control.

Sinónimo: Computación en la nube

2.3.10. Confidencialidad

Definición:
Confidencialidad es la propiedad de la información, por la que se garantiza que está accesible únicamente a personal autorizado a acce-

der a dicha información.

La confidencialidad de la información constituye la piedra angular de la seguridad de la información. Junto con la integridad y la disponibilidad suponen las tres dimensiones de la seguridad de la información.

2.3.11. Control parental

Definición:
Conjunto de herramientas o medidas que se pueden tomar para evitar que los menores de edad hagan un uso indebido del ordenador, accedan a contenidos inapropiados o se expongan a riesgos a través de Internet.

Estas herramientas tienen la capacidad de bloquear, restringir o filtrar el acceso a determinados contenidos o programas, accesibles a través de un ordenador o de la red, y de dotar de un control sobre el equipo y las actividades que se realizan con él, a la persona que sea el administrador del mismo, que normalmente deberá ser el padre o tutor del menor.

Sinónimo: Control paterno

2.3.12. Cookie

Definición:
Una *cookie* es un pequeño fichero que almacena información enviada por un sitio web y que se almacena en el equipo del usuario, de manera que el sitio web puede consultar la actividad previa del usuario.
Sus principales funciones son:

- Llevar el control de usuarios: cuando un usuario introduce su nombre de usuario y contraseña, se almacena una *cookie* para que no tenga que estar introduciéndolas para cada página del servidor.
- Recabar información sobre los hábitos de navegación del usuario. Esto puede significar una ataque contra la privacidad de los usuarios y es por lo que hay que tener cuidado con ellas.

2.3.13. Cortafuegos

Definición:
Sistema de seguridad compuesto o bien de programas (*software*) o de dispositivos *hardware* situados en los puntos limítrofes de una red que tienen el objetivo de permitir y limitar, el flujo de tráfico entre los diferentes ámbitos que protege sobre la base de un conjunto de normas y otros criterios.

La funcionalidad básica de un cortafuego es asegurar que todas las comunicaciones entre la red e Internet se realicen conforme a las políticas de seguridad de la organización o corporación.

Estos sistemas suelen poseer características de privacidad y autentificación.

Sinónimo: *Firewall*

2.3.14. Criptografía

Definición:
La criptografía es la técnica que consiste en cifrar un mensaje, conocido como texto en claro, convirtiéndolo en un mensaje cifrado o criptograma, que resulta ilegible para todo aquel que no conozca el sistema mediante el cual ha sido cifrado.

Existen dos tipos principales de criptografía: por un lado, la conocida como criptografía simétrica, más tradicional, y la criptografía asimétrica o de clave pública.

2.3.15. CRL

Definición:
Cuando una autoridad de certificación emite un certificado digital, lo hace con un periodo máximo de validez (por ejemplo cuatro años).

El objetivo de este periodo de caducidad es obligar a la renovación del certificado para adaptarlo a los cambios tecnológicos. Así se disminuye el riesgo de que el certificado quede comprometido por un avance tecnológico. La fecha de caducidad viene indicada en el propio certificado digital.

Existen otras situaciones que pueden invalidar el certificado digital, de manera inesperada, aun cuando no ha caducado oficialmente:

- robo de la clave privada del usuario del certificado
- desaparece la condición por la que el certificado fue expedido
- el certificado contiene información errónea o información que ha cambiado
- una orden judicial

Por tanto, debe existir algún mecanismo para comprobar la validez de un certificado antes de su caducidad. Las CRL son uno de estos mecanismos.

Las CRL o Listas de revocación de Certificados, es un mecanismo que permite verificar la validez de un certificado digital a través de listas emitidas por las autoridades oficiales de certificación.

Las listas de revocación de certificados incluyen los números de serie de todos los certificados que han sido revocados. Estas listas se actualizan cada 24 horas y pueden ser consultadas a través de Internet.

2.3.16. Códigos de conducta

Definición:
En el ámbito de las TIC, los códigos de conducta son aquellas recomendaciones o reglas que tienen por finalidad determinar las normas deontológicas aplicables en el ámbito de la tecnología y la informática con el objeto de proteger los derechos fundamentales de los usuarios.

Los códigos de conducta se plantean en un ámbito de aplicación muy extenso, sin embargo, desde el punto de vista tecnológico e informático se puede considerar que implican la sujeción a un conjunto de normas y principios éticos cuyo uso y funcionamiento deberá garantizar la plena confianza y seguridad, evitando la vulneración de los derechos de los ciudadanos.

En definitiva, un código de conducta es un conjunto de normas y obligaciones que asumen las personas y entidades que se adscriben al mismo y mediante las cuales se pretende fo-

mentar la confianza y la seguridad jurídica, así como una mejor tramitación de cualquier problema o incidencia.

2.4. D

2.4.1. Denegación de servicio

Definición:
Se entiende como denegación de servicio, en términos de seguridad informática, a un conjunto de técnicas que tienen por objetivo dejar un servidor inoperativo. Mediante este tipo de ataques se busca sobrecargar un servidor y de esta forma impedir que los usuarios legítimos puedan utilizar los servicios por prestados por él.

El ataque consiste en saturar con peticiones de servicio al servidor, hasta que éste no puede atenderlas, provocando su colapso.

Un método más sofisticado es el ataque de Denegación de Servicio Distribuido (DDoS), mediante el cual las peticiones son enviadas, de forma coordinada entre varios equipos, que pueden estar siendo utilizados para este fin sin el conocimiento de sus legítimos dueños (por ejemplo a través de una botnet).

Esto puede ser así mediante el uso de programas *malware* que permitan la toma de control del equipo de forma remota, como puede ser en los casos de ciertos tipos de gusano o bien porque el atacante se ha encargado de entrar directamente en el equipo de la víctima.

Sinónimo: DoS, Ataque de Denegación de Servicio, DDoS

2.4.2. Desbordamiento de búfer

Definición:
Es un tipo de vulnerabilidad muy utilizada con la que se persigue conseguir acceso remoto al sistema atacado. Un desbordamiento de búfer intenta aprovechar defectos en la programación que provocan un error o el cuelgue del sistema. Un desbordamiento de búfer provoca algo similar a lo que ocurre cuando llenamos un vaso más allá de su capacidad: éste se desborda y el contenido se derrama. Cuando el programador no incluye las medidas necesarias para comprobar el tamaño del búfer en relación con el volumen de datos que tiene que alojar, se produce también el derramamiento de estos datos que se sobrescriben en otros puntos de la memoria, lo cual puede hacer que el programa falle.

El atacante calcula qué cantidad de datos necesita enviar y dónde se reescribirán los datos, para a continuación enviar comandos que se ejecutarán en el sistema.

Este tipo de vulnerabilidad, dado que se produce por un defecto en el código del programa, sólo puede ser solventada mediante las actualizaciones o parches del programa en cuestión. Por esta razón es imprescindible mantener actualizados todos los programas instalados en nuestros equipos y servidores.

Sinónimo: *Buffer overflow*

2.4.3. Dirección IP

Definición:
Las direcciones IP (del acrónimo inglés IP para Internet Protocol) son un número único e irrepetible con el cual se identifica a todo sistema conectado a una red.

Podríamos compararlo con una matrícula en un coche. Así, una dirección IP (o simplemente IP) en su versión v4 es un conjunto de cuatro números del 0 al 255 separados por puntos. Por ejemplo: 192.168.121.40

En su versión v6, las direcciones IP son mucho más complejas, siendo hasta 4 veces más largas, más seguras y permitiendo un gran número de sistemas conectados a Internet. Un ejemplo es el siguiente: 2001:0db8:3c4d:0015:0000:0000:1a2f:1a2b

Las direcciones IP pueden ser «públicas», si son accesibles directamente desde cualquier sistema conectado a Internet o «privadas», si son internas a una red LAN y solo accesibles desde los equipos conectados a esa red privada.

Sinónimo: IP

2.4.4. Dirección MAC

Definición:
Una dirección MAC, también conocida como dirección física, es un valor de 48 bits único e irrepetible que identifica todo dispositivo conectado a una red. Cada dispositivo tiene su propia dirección MAC determinada que es única a nivel mundial ya que es escrita directamente, en forma binaria, en el hardware del interfaz de red en el momento de su fabricación.

El acrónimo MAC hace referencia a *Media Access Control* que traducido al español significa Control de Acceso al Medio.

Sinónimo: dirección física, dirección *hardware*

2.4.5. Disponibilidad

Definición:
Se trata de la capacidad de un servicio, un sistema o una información, a ser accesible y utilizable por los usuarios o procesos autorizados cuando éstos lo requieran.

Junto con la integridad y la confidencialidad son las tres dimensiones de la seguridad de la información.

2.4.6. DNS

Definición:
El término DNS, del inglés *Domain Name Service*, se refiere tanto al servicio de Nombres de Dominio, como al servidor que ofrece dicho servicio.

El servicio DNS asocia un nombre de dominio con información variada relacionada con ese dominio. Su función más importante es traducir nombres inteligibles para las personas en direcciones IP asociados con los sistemas conectados a la red con el propósito de poder localizar y direccionar estos sistemas de una forma mucho más simple.

2.5. E

2.5.1. e-administración

Definición:
Véase: Administración electrónica

2.5.2. Exploit

Definición:
Secuencia de comandos utilizados para, aprovechándose de un fallo o vulnerabilidad en un sistema, provocar un comportamiento no deseado o imprevisto. Mediante la ejecución de *exploit* se suele perseguir:

- el acceso a un sistema de forma ilegítima
- obtención de permisos de administración en un sistema ya accedido
- un ataque de denegación de servicio a un sistema

2.6. F

2.6.1. Firma electrónica

Definición:
La firma electrónica (o digital) se define como el conjunto de datos electrónicos que acompañan o que están asociados a un documento electrónico. Esta firma se basa en la Ley 59/2003, de 19 de Diciembre, donde se indica que la «firma electrónica» reconocida debe cumplir las siguientes propiedades o requisitos:

- identificar al firmante
- verificar la integridad del documento firmado
- garantizar el no repudio en el origen
- contar con la participación de un tercero de confianza
- estar basada en un certificado electrónico reconocido
- debe de ser generada con un dispositivo seguro de creación de firma

Una firma electrónica de un documento se consigue calculando el valor «*hash*» del documento y adjuntándolo al final del mismo, para a continuación cifrarlo con la clave pública de la persona a la que enviaremos el documento.

De esta manera nadie pueda leerlo más que el receptor.

Sinónimo: Firma digital

2.6.2. Fuga de datos

Definición:
La fuga de datos o fuga de información es la pérdida de la confidencialidad de la información privada de una persona o empresa. Información que, a priori, no debería ser conocida más que por un grupo de personas, en el ámbito de una organización, área o actividad, y que termina siendo visible o accesible para otros.

Sinónimo: Fuga de información

2.6.3. FTP

Definición:
Por FTP (del acrónimo inglés *File Transfer Protocol*) se hace referencia a un servicio de transferencia de ficheros a través de una red, así como a los servidores que permiten prestar este servicio.

Mediante este servicio, desde un equipo cliente se puede conectar a un servidor para descargar archivos desde él o para enviarle archivos, independientemente del sistema operativo utilizado en cada equipo.

2.7. G

2.7.1. Gusano

Definición:
Es un programa malicioso (o *malware*) que tiene como característica principal su alto grado de «dispersabilidad», es decir, lo rápidamente que se propaga.

Mientras que los troyanos dependen de que un usuario acceda a una web maliciosa o ejecute un fichero infectado, los gusanos realizan copias de sí mismos, infectan a otros ordenadores y se propagan automáticamente en una red independientemente de la acción humana.

Su fin es replicarse a nuevos sistemas para infectarlos y seguir replicándose a otros equipos informáticos, aprovechándose de todo tipo de medios como el correo electrónico, IRC, FTP, correo electrónico, P2P y otros protocolos específicos o ampliamente utilizados.

Sinónimo: *Worm*

2.8. H

2.8.1. HTTP

Definición:
HTTP son las siglas en inglés de Protocolo de Transferencia de Hipertexto. Se trata del protocolo más utilizado para la navegación web. Se trata de un protocolo que sigue un esquema petición-respuesta. El navegador realiza peticiones de los recursos que necesita (la web, las imágenes, los videos…) y el servidor se los envía si dispone de ellos. A cada pieza de información transmitida se la identifica mediante un identificador llamado URL (del inglés *Uniform Resource Locator).*

La información enviada mediante HTTP se envía en texto claro, lo que quiere decir que cualquiera que intercepte el tráfico de red puede leer lo que se está enviando y recibiendo. Por esta razón se desarrolló el protocolo HTTPS, en el que la información es cifrada antes de ser enviada por la red.

2.8.2. HTTPS

Definición:
Protocolo seguro de transferencia de hipertexto, más conocido por sus siglas HTTPS, del inglés *Hypertext Transfer Protocol Secure*, es un protocolo de red basado en el protocolo HTTP,

destinado a la transferencia segura de datos de hipertexto. Dicho en otras palabras, es la versión segura de HTTP.

En HTTPS el tráfico HTTP es cifrado mediante un algoritmo de cifrado simétrico cuya clave ha sido previamente intercambiada entre el navegador y el servidor. Es utilizado por cualquier tipo de servicio que requiera el envío de datos personales o contraseñas, entidades bancarias, tiendas en línea, pago seguro, etc.

2.9. I

2.9.1. IDS

Definición:
Un sistema de detección de intrusos (o IDS de sus siglas en inglés *Intrusion Detection System*) es una aplicación usada para detectar accesos no autorizados a un ordenador o a una red.

Estos accesos pueden ser ataques realizados por usuarios malintencionados con conocimientos de seguridad o usando herramientas automáticas. A diferencia de los IPS, estos sistemas sólo detectan intentos de acceso y no tratan de prevenir su ocurrencia.

2.9.2. Incidente de seguridad

Definición:
Cualquier suceso que afecte a la confidencialidad, integridad o disponibilidad de los activos de información de la empresa, por ejemplo: acceso o intento de acceso a los sistemas, uso, divulgación, modificación o destrucción no autorizada de información.

2.9.3. Informática forense

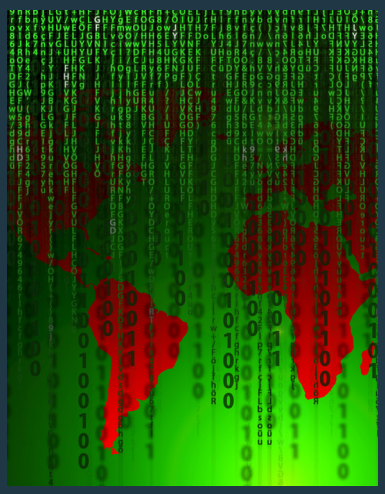
Definición:
La informática forense consiste en un proceso de investigación de los sistemas de información para detectar toda evidencia que pueda ser presentada como prueba fehaciente en un procedimiento judicial.

Para esta investigación se hace necesaria la aplicación de técnicas científicas y analíticas especializadas que permitan identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal. Entre las técnicas mencionadas se incluyen reconstruir el sistema informático, examinar datos residuales y explicar las características técnicas del uso aplicado a los datos y bienes informáticos.

Su implementación debe llevarse a cabo considerando lo dispuesto por la normativa legal aplicable, a efectos de no vulnerar los derechos de protección de datos y de intimidad de terceros.

Los principales objetivos de la informática forense son:

- Utilización de técnicas que garanticen la seguridad de la información corporativa, como medida preventiva.
- Reunir las evidencias electrónicas como medio probatorio para detectar el origen de un ataque.
- Garantizar los requerimientos técnicos y jurídicos de los sistemas de seguridad de la información.



« El malware tiene como objetivo dañar o infiltrarse sin el consentimiento de su propietario en un sistema de información»

Sinónimo: Análisis forense digital

2.9.4. Infraestructura de clave pública

Definición:
También conocido por las siglas PKI (del inglés *Public Key Infrastructure*), una infraestructura de clave pública es un conjunto de elemento Hardware, Software, políticas y procedimientos de actuación encaminados a la ejecución con garantías de operaciones de cifrado y criptografía, tales la firma, el sellado temporal o el no repudio de transacciones electrónicas.

Sinónimo: PKI

2.9.5. Ingeniería social

Definición:
Las técnicas de ingeniería social son tácticas utilizadas para obtener información datos de naturaleza sensible, en muchas ocasiones claves o códigos, de una persona. Estas técnicas de persuasión suelen valerse de la buena voluntad y falta de precaución de la víctima.

2.9.6. Integridad

Definición:
La Integridad es la propiedad de la información, por la que se garantiza la exactitud de los datos transportados o almacenados, asegurando que no se ha producido su alteración, pérdida o destrucción, ya sea de forma accidental o intencionada, por errores de *software* o *hardware* o por condiciones medioambientales. La integridad, la disponibilidad y la confidencialidad constituyen las dimensiones claves en la seguridad de la información, ya que de un lado, se pretende evitar los accesos no autorizados a los datos, y de otro, se garantiza la no alteración de los mismos.

2.9.7. Inyección SQL

Definición:
Es un tipo de ataque que se aprovecha de una vulnerabilidad en la validación de los contenidos introducidos en un formulario web y que puede permitir la obtención de forma ilegítima de los datos almacenados en la base de datos del sitio web, entre ellos las credenciales de acceso.

Sinónimo: SQL *Injection*

2.9.8. IPS

Definición:
Siglas de *Intrusion Prevention System* (sistema de prevención de intru-

siones). Es un *software* que se utiliza para proteger a los sistemas de ataques y abusos. La tecnología de prevención de intrusos puede ser considerada como una extensión de los sistemas de detección de intrusos (IDS), pero en realidad es una tecnología más cercana a los cortafuegos.

2.10. L

2.10.1. LAN

Definición:
Una LAN (del inglés *Local Area Network*) o Red de Área Local es una red informática de pequeña amplitud geográfica, que suele limitarse a espacios como una oficina, una vivienda o un edificio. Una Red de Área Local permite interconectar distintos dispositivos todo tipo, ordenadores, impresoras, servidores, discos duros externos, etc.

Las Redes de Área Local pueden ser cableadas o no cableadas, también conocidas como redes inalámbricas. Por término general las redes cableadas son más rápidas y seguras, pero impiden la movilidad de los dispositivas.

Sinónimo: Red de Área Local

2.11. M

2.11.1. Malware

Definición:
Es un tipo de *software* que tiene como objetivo dañar o infiltrarse sin el consentimiento de su propietario en un sistema de información. Palabra que nace de la unión de los términos en inglés de *software* malintencionado: *malicious software*.

Dentro de esta definición tiene cabida un amplio elenco de programas maliciosos: virus, gusanos, troyanos, *backdoors*, *spyware*, etc. La nota común a todos estos programas es su carácter dañino o lesivo.

Sinónimo: *Software* malicioso

2.11.2. Malvertising

Definición:
Véase: *Adware*

2.11.3. Metadatos

Definición:
Los metadatos son el conjunto de datos relacionados con un documento y que recogen información fundamentalmente descriptiva del mismo, así como información de administración y gestión. Los metadatos es una información que enriquece el documento al que está asociado.

A modo de ejemplo, se podría considerar como una analogía al uso de índices que se emplean en una biblioteca, donde gracias a datos del tipo: autor, títulos, etcétera se nos permite localizar un libro en concreto.

Otro ejemplo de uso es mejorar las consultas en los buscadores consiguiendo una mayor exactitud y precisión en los resultados.

2.12. N

2.12.1. No repudio

Definición:
El no repudio en el envío de información a través de las redes es capacidad de demostrar la identidad del emisor de esa información. El objetivo que se pretende es certificar que los datos, o la información, provienen realmente de la fuente que dice ser.

El problema del control de autenticidad dentro de los sistemas de información a través de la Red, en relación tanto de la identidad del sujeto como del contenido de los datos, puede ser resuelto mediante la utilización de la firma electrónica (o digital).

Sinónimo: Autenticidad

2.13. P

2.13.1. P2P

Definición:
P2P (del inglés *Peer-to-Peer*) es un modelo de comunicaciones entre sistemas o servicios en el cual todos los nodos/extremos son iguales, tienen las mismas capacidades y cualquiera de ellas puede iniciar la comunicación.

Se trata de un modelo opuesto al cliente/servidor en donde el servidor se encuentra a la espera de una comunicación por parte del cliente. El modelo P2P se basa en que todos los nodos actúan como servidores y clientes a la vez.

Una red P2P es por tanto una red de sistemas o servicios que utiliza un modelo P2P. Todos los sistemas/servicios conectados entre sí y que se comportan como iguales con un objetivo en común.

Por ejemplo las botnets P2P utilizan este modelo para evitar que haya un servidor central único fácilmente detectable.

Sinónimo: Red P2P

2.13.2. Parche de seguridad

Definición:
Un parche de seguridad es un conjunto de cambios que se aplican a un *software* para corregir errores de seguridad en programas o sistemas operativos. Generalmente los parches de seguri-

dad son desarrollados por el fabricante del *software* tras la detección de una vulnerabilidad en el *software* y pueden instalarse de forma automática o manual por parte del usuario.

Sinónimo: Actualización de seguridad

2.13.3. Pentest

Definición:
Una prueba de penetración es un ataque a un sistema *software* o *hardware* con el objetivo de encontrar vulnerabilidades. El ataque implica un análisis activo de cualquier vulnerabilidad potencial, configuraciones deficientes o inadecuadas, tanto de *hardware* como de *software*, o deficiencias operativas en las medidas de seguridad.

Este análisis se realiza desde la posición de un atacante potencial y puede implicar la explotación activa de vulnerabilidades de seguridad.

Tras la realización del ataque se presentará una evaluación de seguridad del sistema, indicando todos los problemas de seguridad detectados junto con una propuesta de mitigación o una solución técnica.

La intención de una prueba de penetración es determinar la viabilidad de un ataque y el impacto en el negocio de un ataque exitoso.

Sinónimo: Prueba de penetración

2.13.4. PCI DSS

Definición:
PCI DSS (del Inglés *Payment Card Industry Data Security Standard*) es, como su nombre indica un Estándar de Seguridad de Datos para la Industria de Tarjetas de Pago.

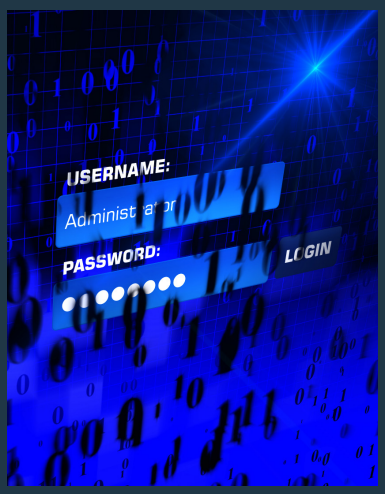
Este estándar ha sido desarrollado por un comité conformado por las compañías de tarjetas (débito y crédito) más importantes, comité denominado PCI SSC (*Payment Card Industry Security Standards Council*) como una guía que ayude a las organizaciones que procesan, almacenan o transmiten datos de tarjetas (o titulares de tarjeta), a asegurar dichos datos, con el fin de prevenir los fraudes que involucran tarjetas de pago débito y crédito.

2.13.5. Pharming

Definición:
Ataque informático que aprovecha una vulnerabilidad del *software* de los servidores DNS y que consiste en modificar o sustituir el archivo del servidor de nombres de dominio cambiando la dirección IP legítima de una entidad (comúnmente una entidad bancaria) de manera que en el momento en el que el usuario escribe el nombre de dominio de la entidad en la barra de direcciones, el navegador redirigirá automáticamente al usuario a una dirección IP donde se aloja una web falsa que suplantará la identidad legítima de la entidad, obteniéndose de forma ilícita las claves de acceso de los clientes la entidad.

2.13.6. Phishing

Definición:



« La política de seguridad decide las medidas de seguridad que una empresa toma respecto a sus sistemas de información»

Phishing es la denominación que recibe la estafa cometida a través de medios telemáticos mediante la cual el estafador intenta conseguir, de usuarios legítimos, información confidencial (contraseñas, datos bancarios, etc.) de forma fraudulenta.

El estafador o *phisher* suplanta la personalidad de una persona o empresa de confianza para que el receptor de una comunicación electrónica aparentemente oficial (vía e-mail, fax, SMS o telefónicamente) crea en su veracidad y facilite, de este modo, los datos privados que resultan de interés para el estafador.

Existen diferentes modalidades de *phishing*. Cuando éste se realiza vía SMS el nombre técnico es *Smishing* y cuando se realiza utilizando Voz sobre IP, se denomina *vishing*. Otra variedad es el *spear phishing*, en la que los atacantes intentan mediante un correo electrónico, que aparenta ser de un amigo o de empresa conocida, conseguir que les facilitemos: información financiera, números de tarjeta de crédito, cuentas bancarias o contraseñas.

Sinónimo: *Vishing, Smishing, Spear phishing*

2.13.7. PGP

Definición:
Pretty Good Privacy, más conocido como PGP, es un programa para proteger la información transmitida por internet mediante el uso de criptografía de clave pública, así como facilitar la autenticación de documentos mediante firma electrónica. PGP protege no solo los datos durante su tránsito por la Red, como para proteger archivos almacenados en disco. PGP goza de gran popularidad por su facilidad de uso y por su alto nivel de fiabilidad.

El estándar de Internet OpenPGP, basado en PGP, es uno de los estándares de cifrado de correo electrónico más utilizados.

2.13.8. Plan de contingencia

Definición:
Un Plan de Contingencia de las Tecnologías de la Información y las Comunicaciones (TIC) consiste en una estrategia planificada en fases, constituida por un conjunto de recursos de respaldo, una organización de emergencia y unos procedimientos de actuación, encaminados a conseguir una restauración ordenada, progresiva y ágil de los sistemas de información que soportan la información y los procesos de negocio considerados críticos en el Plan de Continuidad de Negocio de la compañía.

2.13.9. Plan de continuidad

Definición:
Un Plan de Continuidad de Negocio es un conjunto formado por planes de actuación, planes de emergencia, planes financieros, planes de comunicación y planes de contingencias destinados a mitigar el impacto provocado por la concreción de determinados riesgos sobre la información y los procesos de negocio de una compañía.

Sinónimo: BCP

2.13.10. Política de seguridad

Definición:
Son las decisiones o medidas de seguridad que una empresa ha decidido tomar respecto a la seguridad de sus sistemas de información después de evaluar el valor de sus activos y los riegos a los que están expuestos.

Este término también se refiere al documento de nivel ejecutivo mediante el cual una empresa establece sus directrices de seguridad de la información.

2.13.11. Protocolo

Definición:
Es un sistema de reglas que permiten que dos o más entidades se comuniquen entre ellas para transmitir información por medio de cualquier tipo de medio físico.

Se trata de las reglas o el estándar que define la sintaxis, semántica y sincronización de la comunicación, así como también los posibles métodos de recuperación de errores.

Los protocolos pueden ser implementados por *hardware*, por *software*, o por una combinación de ambos.

2.13.12. Proveedor de acceso

Definición:
Se denomina proveedor de acceso (a Internet) a todos los prestadores de servicios de la Sociedad de la Información que proporcionan a sus usuarios/clientes acceso a redes de telecomunicaciones, tanto fijas como móviles.

En inglés se denomina ISP, acrónimo de *Internet Service Provider.*

Sinónimo: ISP

2.13.13. Proxy

Definición:
El *proxy* es tanto el equipo, como el *software* encargado de dar el servicio, que hacen de intermediario en las peticiones de los equipos de la redes LAN hacia Internet.

Su cometido es de centralizar el tráfico entre Internet y una red privada, de forma que se evita que cada una de las máquinas de la red privada tenga que disponer necesariamente de una conexión directa a Internet y una dirección IP pública.
A mismo tiempo un *proxy* puede proporcionar algunos mecanismos de seguridad (*firewall*

o cortafuegos) que impiden accesos no autorizados desde el exterior hacia la red privada.

Sinónimo: *Gateway*

2.13.14. Puerta trasera

Definición:
Se denomina *backdoor* o puerta trasera a cualquier punto débil de un programa o sistema mediante el cual una persona no autorizada puede acceder a un sistema.

Las puertas traseras pueden ser errores o fallos, o pueden haber sido creadas a propósito, por los propios autores pero al ser descubiertas por terceros, pueden ser utilizadas con fines ilícitos.

Por otro lado, también se consideran puertas traseras a los programas que, una vez instalados en el ordenador de la víctima, dan el control de éste de forma remota al ordenador del atacante. Por lo tanto aunque no son específicamente virus, pueden llegar a ser un tipo de malware que funcionan como herramientas de control remoto. Cuentan con una codificación propia y usan cualquier servicio de Internet: correo, mensajería instantánea, http, ftp, telnet o chat. Chat.

Sinónimo: *Backdoor*

2.14. R

2.14.1. Ransomware

Definición:
El ciberdelincuente, toma control del equipo infectado y «secuestra» la información del usuario cifrándola, de tal forma que permanece ilegible si no se cuenta con la contraseña de descifrado. De esta manera extorsiona al usuario pidiendo un rescate económico a cambio de esta contraseña para que, supuestamente, pueda recuperar sus datos.

La seguridad del sistema está basada en la dificultad de factorización de grandes números. Su funcionamiento se basa en el envío de un mensaje cifrado mediante la clave pública del destinatario, y una vez que el mensaje cifrado llega, éste se encarga de descifrarlo con su clave privada.

2.14.2. Red privada virtual

Definición:
Una red privada virtual, también conocida por sus siglas VPN (*Virtual Private Network*) es una tecnología de red que permite una extensión segura de una red local (LAN) sobre una red pública o no controlada como Internet.

Al establecerlas, la integridad de los datos y la confidencialidad se protegen mediante la autentificación y el cifrado.

Se trata realmente de una conexión virtual punto a punto entre dos redes LAN usando para la conexión una red pública como es Internet y consiguiendo que esta conexión sea segura gracias al cifrado de la comunicación.

Sinónimo: VPN

2.14.3. RFID

Definición:
Siglas de *Radio Frequency IDentification*, en español Identificación por Radiofrecuencia. Como su nombre indica es un método de identificación de dispositivos por ondas de radio.

El propósito fundamental de la tecnología RFID es transmitir la identidad de un objeto (similar a un número de serie único) de una forma inalámbrica.

Las etiquetas RFID (RFID Tag, en inglés) son unos dispositivos pequeños, similares a una pegatina, que pueden ser adheridas o incorporadas a un producto y que contienen una mini-antena que les permitirles recibir y responder a peticiones por radiofrecuencia desde un lector RFID.

RFID se utiliza en muchos ámbitos, por ejemplo los arcos de detección en las entradas de las tiendas o los controles de acceso mediante tarjeta por proximidad.

2.14.4. Router

Definición:
Es un dispositivo que distribuye tráfico de red entre dos o más diferentes redes. Un router está conectado al menos a dos redes, generalmente LAN o WAN y el tráfico que recibe procedente de una red lo redirige hacia la(s) otra(s) red(es).

En términos domésticos un router es el dispositivo que proporciona el proveedor de servicios de telefonía (o ISP) y que permite conectar nuestra LAN doméstica con la red del IS.

El router comprueba las direcciones de destino de los paquetes de información y decide por qué ruta serán enviados, para determinar el mejor camino emplean cabeceras y tablas de comparación.

Sinónimo: Enrutador, Encaminador, Rúter

2.14.5. RSA

Definición:
Se trata de un sistema criptográfico de clave pública desarrollado por los criptógrafos Rivest, Shamir y Adleman, de donde toma su nombre.

Es el primer y más utilizado algoritmo de este tipo y permite tanto cifrar documentos como firmarlos digitalmente.

2.15. S

2.15.1. SaaS

Definición:
Son las siglas de *Software as a Service*, es decir la utilización de *Software* como un servicio.

Es un modelo de distribución de *software* donde tanto el *software* como los datos que maneja se alojan en servidores de un tercero (generalmente el fabricante del *software*) y el cliente accede a los mismos vía Internet.

2.15.2. Servidor

Definición:
Puede entenderse como servidor tanto el *software* que realiza ciertas tareas en nombre de los usuarios, como el ordenador físico en el cual funciona ese *software*, una máquina cuyo propósito es proveer y gestionar datos de algún tipo de forma que estén disponibles para otras máquinas que se conecten a él.

Así, se entiende por servidor tanto el equipo que almacena una determinada información como el programa de software encargado de gestionar dicha información y ofrecerla.

Algunos ejemplos de servidores son los que proporcionan el alojamiento de sitios web y los que proporcionan el servicio de envío, reenvío y recepción de correos electrónicos.

2.15.3. SGSI

Definición:
Un Sistema de Gestión de la seguridad de la Información (SGSI) es un conjunto de políticas de seguridad de la información que siguen la norma ISO/IEC 27001.

Un SGSI es para una organización el diseño, implantación, mantenimiento de un conjunto de procesos para gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información minimizando a la vez los riesgos de seguridad de la información.

2.15.4. Sistemas de reputación

Definición:
En los servicios de compraventa online se suelen adoptar sistemas de reputación. Estos sistemas permiten conocer la opinión de otros compradores y sus experiencias para valorar si el sitio merece nuestra confianza.

Estos sistemas permiten que los usuarios que han utilizado un servicio de compraventa online publiquen sus opiniones y experiencias con éste y califiquen el servicio. A partir de esta información, nosotros podemos hacernos una idea del nivel de confianza, seguridad y garantía que podemos obtener del servicio si decidimos utilizarlo.

Estos sistemas son ventajosos tanto para los propietarios de los servicios de compraventa online como para sus usuarios, por esto, no es de extrañar que las páginas especializadas en compraventa, subastas y venta por Internet demuestren su interés en utilizarlos.
Otro ejemplo de sistema de reputación son las listas negras que valoran si una dirección IP son emisoras de spam o que valoran si una dirección IP aloja *phishing*. Estos sistemas de reputación ayudan a evitar ser víctimas de *spam* o *phishing*.

2.15.5. SLA

Definición:
Un acuerdo de nivel de servicio o ANS (en inglés *Service Level Agreement* o SLA), es un contrato escrito entre un proveedor de servicio y su cliente con objeto de fijar el nivel acordado para la calidad de dicho servicio.

El ANS es una herramienta que ayuda a ambas partes a llegar a un consenso en términos del

nivel de calidad del servicio, en aspectos tales como tiempo de respuesta, disponibilidad horaria, documentación disponible, personal asignado al servicio, etc.

Sinónimo: Acuerdo de Nivel de Servicio

2.15.6. SMTP

Definición:
El Protocolo Simple de Transferencia de Correo (o *Simple Mail Transfer Protocol* del inglés) es un protocolo de red utilizado para el intercambio de mensajes de correo electrónico.

Este protocolo, aunque es el más comúnmente utilizado, posee algunas limitaciones en cuanto a la recepción de mensajes en el servidor de destino (cola de mensajes recibidos).

Como alternativa a esta limitación crearon los protocolos POP o IMAP, otorgando a SMTP la tarea específica de enviar correo, y recibirlos empleando los otros protocolos antes mencionados (POP O IMAP).

2.15.7. Sniffer

Definición:
Un *sniffer* es un programa que monitoriza la información que circula por la red con el objeto de capturar información.

Las tarjetas de red pueden verificar si la información recibida está dirigida o no a su sistema.

Si no es así, la rechaza. Un *sniffer* lo que hace es colocar a la placa de red en un modo el cual desactiva el filtro de verificación de direcciones (promiscuo) y por lo tanto acepta todos los paquetes que llegan a la tarjeta de red del ordenador donde está instalado estén dirigidos o no a ese dispositivo.

El tráfico que no viaje cifrado podrá por tanto ser «escuchado» por el usuario del *sniffer*.

El análisis de tráfico puede ser utilizado también para determinar relaciones entre varios usuarios (conocer con qué usuarios o sistemas se relaciona alguien en concreto).

No es fácil detectar si nuestro tráfico de red está siendo «escuchado» mediante un *sniffer*, por lo que siempre es recomendable utilizar tráfico cifrado en todas las comunicaciones.

2.15.8. Spoofing

Definición:
Es una técnica de suplantación de identidad en la Red, llevada a cabo por un ciberdelincuente generalmente gracias a un proceso de investigación o con el uso de *malware*. Los ataques de seguridad en las redes usando técnicas de *spoofing* ponen en riesgo la privacidad de los usuarios, así como la integridad de sus datos.

De acuerdo a la tecnología utilizada se pueden diferenciar varios tipos de *spoofing*:

- IP *spoofing*: consiste en la suplantación de la dirección IP de origen de un paquete TCP/IP por otra dirección IP a la cual se desea suplantar.
- ARP *spoofing*: es la suplantación de identidad por falsificación de tabla ARP. ARP (*Address Resolution Protocol*) es un protocolo de nivel de red que relaciona una dirección

MAC con la dirección IP del ordenador. Por lo tanto, al falsear la tabla ARP de la víctima, todo lo que se envíe a un usuario, será direccionado al atacante.
• DNS *spoofing*: es una suplantación de identidad por nombre de dominio, la cual consiste en una relación falsa entre IP y nombre de dominio.
• Web *spoofing*: con esta técnica el atacante crea una falsa página web, muy similar a la que suele utilizar el afectado con el objetivo de obtener información de dicha víctima como contraseñas, información personal, datos facilitados, páginas que visita con frecuencia, perfil del usuario, etc. Los ataques de *phishing* son un tipo de Web *spoofing*.
• Mail *spoofing*: suplantación de correo electrónico bien sea de personas o de entidades con el objetivo de llevar a cabo envío masivo de *spam*.

2.15.9. Spyware

Definición:
Es un *malware* que recopila información de un ordenador y después la envía a una entidad remota sin el conocimiento o el consentimiento del propietario del ordenador.

El término *spyware* también se utiliza más ampliamente para referirse a otros productos como *adware*, falsos antivirus o troyanos.

Sinónimo: Programa espía

2.15.10. SSL

Definición:
Es un protocolo criptográfico seguro que proporciona comunicaciones seguras a través de una red (por ejemplo Internet). Generalmente comunicaciones cliente-servidor. El uso de SSL (*Secure Sockets Layer*) proporciona autenticación y privacidad de la información entre extremos sobre una red mediante el uso de criptografía.

SSL garantiza la confidencialidad de la información utilizando una clave de cifrado simétrica y para garantizar la autenticación y seguridad de la clave simétrica, se utilizan algoritmos de cifrado asimétrico y certificados X.509.

En comunicaciones SSL de forma general solo se autentica el lado del servidor mientras que el cliente se mantiene sin autenticar; la autenticación mutua requiere un despliegue de infraestructura de claves públicas (PKI) para los clientes.

SSL ha evolucionado hacia TLS, siglas en ingles de «seguridad de la capa de transporte» (*Transport Layer Security*) protocolo ampliamente utilizado en la actualidad.

Sinónimo: TLS

2.15.11. Suplantación de identidad

Definición:
Es la actividad maliciosa en la que un atacante se hace pasar por otra persona para cometer algún tipo de fraude, acoso (*cyberbulling*).

Un ejemplo es, en las redes sociales, crear un perfil de otra persona e interactuar con otros usuarios haciéndose pasar por ella.

« Los virus pueden copiarse a sí mismos adjuntándose en aplicaciones existentes en el equipo»

2.16. T

2.16.1. TCP/IP

Definición:
Por TCP/IP se conoce a una familia de protocolos sobre los cuales funciona Internet, permitiendo la comunicación entre todos los servidores conectados a dicha red.

TCP/IP consta entre otros muchos, del protocolo IP (*Internet Protocol*), que se ocupa de transferir los paquetes de datos hasta su destino correcto y el protocolo TCP (*Transfer Control Protocol*), que se ocupa de garantizar que la transferencia se lleve a cabo de forma correcta y confiable.

Entre otros muchos, esta familia consta de los protocolos ICMP, UDP, DNS, HTTP y FTP.

2.16.2. Troyano

Definición:
Se trata de un tipo de *malware* o *software* malicioso que se caracteriza por carecer de capacidad de autoreplicación. Generalmente, este tipo de *malware* requiere del uso de la ingeniería social para su propagación.

Una de las características de los troyanos es que al ejecutarse no se evidencian señales de un mal funcionamiento; sin embargo, mientras el usuario realiza tareas habituales en su ordenador, el programa puede abrir diversos canales de comunicación con un equipo malicioso remoto que permitirán al atacante controlar nuestro sistema de una forma absoluta.

2.17. U

2.17.1. URL

Definición:
Las siglas URL (*Uniform Resource Locator*) hacen referencia a la dirección que identifica un contenido colgado en Internet.

Las URL permiten tener acceso a los recursos colgados en una red gracias a la dirección única y al servicio de DNS que permite localizar la dirección IP del contenido al que se quiere acceder.

2.18. V

2.18.1. Virtualización

Definición:
La virtualización es un medio para crear una versión virtual de un dispositivo o recurso, como un servidor, o una red, en una máquina física, generalmente con el apoyo de un *software* que implementa una capa de abstracción para que la maquina física y la virtual puedan comunicarse y compartir recursos.

2.18.2. Virus

Definición:
Programa diseñado para que al ejecutarse, se copie a sí mismo adjuntándose en aplicaciones existentes en el equipo. De esta manera, cuando se ejecuta una aplicación infectada, puede infectar otros archivos.

A diferencia de otro tipo de *malware*, como los gusanos, se necesita acción humana para que un virus se propague entre máquinas y sistemas.

Los efectos que pueden provocar varían dependiendo de cada tipo de virus: mostrar un mensaje, sobrescribir archivos, borrar archivos, enviar información confidencial mediante correos electrónicos a terceros, etc. Los más comunes son los que infectan a ficheros ejecutables.

2.18.3. VLAN

Definición:
Una red de área virtual o VLAN (acrónimo de *Virtual Local Area Network*) es una red lógica independiente dentro de una red física de forma que es posible crear diferentes una VLAN que este conectadas físicamente a diferentes segmentos de una red de área local o LAN. Los administradores de este tipo de redes las configuran mediante software en lugar de *hardware*, lo que las hace extremadamente flexibles. Esta flexibilidad se hace presente en el hecho de que varias de estas redes pueden coexistir en un solo conmutador o red física.

Otra de las ventajas de este tipo de redes surge cuando se traslada físicamente algún ordenador a otra ubicación ya que no es necesario volver a configurar el *hardware*.

2.18.4. VoIP

Definición:
Señal de voz digitalizada que viaja a través de una red utilizando el protocolo IP (*Internet Protocol*) que es el utilizado en Internet. Esta tecnología permite mantener conversaciones de voz sin necesidad de una conexión telefónica.

La tecnología VoIP utiliza un *software* especial que transforma la voz humana en una señal digital, que es enviada a través de Internet, donde el proceso se invierte para que la persona destinataria pueda escuchar correctamente la voz, tal y como ocurre en la telefonía tradicional.

La principal ventaja de esta tecnología es la importante reducción de los costes que conlleva su uso, así como la portabilidad y la posibilidad de enviar o recibir llamadas de y desde cualquier parte del mundo con un coste mínimo.

2.18.5. VPN

Definición:
Véase: Red Privada Virtual

2.18.6. Vulnerabilidad

Definición:
Fallos o deficiencias de un programa que pueden permitir que un usuario no legítimo acceda a la información o lleve a cabo operaciones no permitidas de manera remota.

Los agujeros de seguridad pueden ser aprovechadas por atacantes mediante exploits, para acceder a los sistemas con fines maliciosos. Las empresas deben ser conscientes de estos riesgos y mantener una actitud preventiva, así como llevar un control de sus sistemas mediante actualizaciones periódicas.

Sinónimo: Agujero de seguridad

2.19. W

2.19.1. Wifi

Definición:
Una red wifi es una red de dispositivos inalámbricos interconectados entre sí y generalmente también conectados a Internet a través de un punto de acceso inalámbrico. Se trata por tanto de una red LAN que no utiliza un cable físico para el envío de la información.

Tecnología de interconexión de dispositivos electrónicos de forma inalámbrica, que funciona en base al estándar 802.11, que regula las transmisiones inalámbricas. Esta ausencia de cable físico quiere decir que se pierda la confidencialidad de la información transmitida. Por esta razón se hace necesario el cifrado de los contenidos transmitidos a través de una red wifi.

Existen generalmente tres sistemas de protección y cifrado de una red wifi:

- WEP
- WPA
- WPA2

Actualmente la única realmente segura de las 3 es WPA2, las otras dos son muy vulnerables y fácilmente descifrables.

Sinónimo: Wi-Fi, WiFi

2.20. X

2.20.1. XSS

Definición:
Se trata de una vulnerabilidad existente en algunas páginas web generadas dinámicamente

(en función de los datos de entrada). XSS viene del acrónimo en inglés de Secuencias de comandos en sitios cruzados (*Cross-site Scripting*).

Dado que los sitios web dinámicos dependen de la interacción del usuario, es posible insertar en un formulario un pequeño programa malicioso, ocultándolo entre solicitudes legítimas y hacer que éste se ejecute. Los puntos de entrada comunes incluyen buscadores, foros, blogs y todo tipo de formularios alojados en una página web.

Una vez realizado el ataque XSS, el atacante puede cambiar la configuración del servidor, secuestrar cuentas, escuchar comunicaciones (incluso cifradas), instalar publicidad en el sitio víctima y en general cualquier acción que desee de forma inadvertida para el administrador.

Sinónimo: Secuencias de comandos en sitios cruzados

2.21. Z

2.21.1. Zero-day

Definición:
Son aquellas vulnerabilidades en sistemas o programas informáticos que son únicamente conocidas por determinados atacantes y son desconocidas por los fabricantes y usuarios. Al ser desconocidas por los fabricantes, no existe un parche de seguridad para solucionarlas.

Por esta razón son muy peligrosas ya que el atacante puede explotarlas sin que el usuario sea consciente de que es vulnerable.

Sinónimo: *0-day*

2.21.2. Zombie

Definición:
Es el nombre que se da a los ordenadores controlados de manera remota por un ciberdelincuente al haber sido infectados por un *malware*.

El atacante remoto generalmente utiliza el ordenador *zombie* para realizar actividades ilícitas a través de la Red, como el envío de comunicaciones electrónicas no deseadas, o la propagación de otro *malware*.

Son sistemas *zombie* los ordenadores que forman parte de una botnet, a los que el bot master utiliza para realizar acciones coordinadas como ataques de denegación de servicio.

Sinónimo: *Bot*

2.22. 0-9

2.22.1. 0-day

Definición:
Véase: *Zero-day*

3. Fuentes de referencia

[1] Symantec Glosario de seguridad. https://www.symantec.com/es/es/security_response/glossary/ (consulta: 02/02/2017)

[2] Panda. Glosario. http://www.pandasecurity.com/spain/homeusers/security-info/glossary/ (consulta: 02/02/2017)

[3] Viruslist. Glosario. https://securelist.com/encyclopedia/ (consulta: 02/02/2017)

[4] Safemode. Glosario. http://safemode-cl.blogspot.com.es/2006/07/glosario-de-terminos-de-seguridad.html (consulta: 02/02/2017)

[5] CERT UY. http://www.cert.uy/inicio/sobre_seguridad/glosario/ (consulta: 02/02/2017)

GOBIERNO DE ESPAÑA
MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL