Glosario de términos de ciberseguridad

Una guía de aproximación para el empresario

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA SEGUNDA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD
017
protege tu empresa

Glosario de términos de ciberseguridad

Una guía de aproximación para el empresario

ÍNDICE

INCIBE_PTE_AproxEmpresario_010_GlosarioCiberseguridad-2020-v2

ÍNDICE

ÍNDICE

ÍNDICE

ÍNDICE

ÍNDICE

ÍNDICE

ÍNDICE

ÍNDICE

1. Introducción

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

Para la definición de los términos se han utilizado las fuentes de referencia, la Wikipedia o el propio portal de INCIBE 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. Actualización de seguridad

Definición:
Modificaciones que se aplican, de forma automática o manual, en el *software* de los sistemas operativos o aplicaciones instalado en los dispositivos electrónicos, con el objetivo de corregir fallos de seguridad, errores de funcionamiento o bien para dotar a los dispositivos de nuevas funcionabilidades, así como incorporar mejoras de rendimiento.

Sinónimo: Parches de seguridad.

2.1.3. 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

2.1.4. 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.

2.1.5. Adware

Definición:
Software que se apoya en anuncios (normalmente para financiarse) como parte del propio programa. En algunos casos se les considera *malware*. Común en las versiones gratuitas en las aplicaciones.

Sinónimo: *Malvertising*

2.1.6. AES

Definición:
Acrónimo en inglés de *Advanced Encryption Standard* (AES); en español, estándar de cifrado avanzado. Es un algoritmo de cifrado de acceso público basado en clave compartida (Algoritmo criptográfico simétrico), en el que, tanto el tamaño de bloque como el de la clave, son fijos.

2.1.7. Agujero de seguridad

Definición:
Véase: Vulnerabilidad

2.1.8. 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.

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

2.1.9. Alta disponibilidad

Definición:
Característica de un sistema o servicio que permite reducir al mínimo el tiempo de indisponibilidad en caso de fallo o incidente; es decir, el tiempo en el que no estará accesible. Este nivel de funcionamiento (o el tiempo máximo de caída) ha de ser acordado entre el proveedor y el cliente en el caso de un servicio, en el marco de un Acuerdo de Nivel de Servicio. Es una funcionalidad necesaria para garantizar los servicios esenciales o imprescindibles de una empresa, cuando esta se enfrenta a incidentes que puedan afectar a su funcionamiento normal o disponibilidad.

2.1.10. 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.

2.1.11. Amenaza avanzada persistente (APT)

Definición:
También conocido como APT, acrónimo en inglés de *Advanced Persistent Threat*, consiste en un tipo de ataque informático que se caracteriza por realizarse con sigilo, permaneciendo activo y oculto durante mucho tiempo, utilizando diferentes formas de ataque. Suelen estar patrocinados por compañías, mafias o un estado. El objetivo principal es vigilar, exfiltrar datos o modificar los recursos de una empresa u organización de forma integrada y continuada en el tiempo. Generalmente, este tipo de *malware* hace uso de *exploits* o ejecutables, aprovechando vulnerabilidades de tipo *Zero Day* presentes en el *software* de la víctima.

2.1.12. 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.

2.1.13. Análisis de vulnerabilidades

Definición:
Consiste en la búsqueda y documentación de fallos, carencias o debilidades físicas (inundaciones, incendios, controles de acceso...) y lógicas (configuraciones, actualizaciones...) en un sistema informático, que puedan ser empleados por terceros con fines ilícitos, suponiendo un riesgo para la organización y los propios sistemas. El análisis propone vías de mitigación a implementar para subsanar las deficiencias encontradas y evitar ataques a los sistemas informáticos.

2.1.14. Análisis heurístico

Definición:
Detección proactiva y autónoma de *malware* u otras amenazas en un sistema, mediante la utilización de técnicas heurísticas; es decir, basadas en la experiencia. Para ello, realizan la comparación de ficheros sospechosos con fragmentos de código de virus de similar comportamiento o detectan actividades sospechosas de un programa por similitud con actividades conocidas de programas maliciosos. El análisis heurístico trata de detectar la presencia de nuevos virus de reciente aparición que aún no han sido documentados por los fabricantes de soluciones de seguridad, y por tanto, no se encuentran aún en la base de datos de los antivirus.

2.1.15. Antispyware

Definición:
Herramienta de *software* diseñada para detectar y eliminar programas maliciosos del tipo *spyware* cuyo objetivo es espiar y obtener de forma sigilosa información personal presente en el dispositivo sin consentimiento del usuario.

2.1.16. Antivirus

Definición:
Software de protección para evitar que ejecutemos algún tipo de *software* malicioso en nuestro equipo que infecte al equipo.

Sinónimo: Antimalware

2.1.17. Ataque activo

Definición:
Tipo de ataque detectable que se caracteriza por la modificación del contenido de la información, así como de los recursos o funcionamiento del sistema, pudiendo causar daños a dicho sistema. Este tipo de ataques pone en riesgo los principios de la seguridad de la información: confidencialidad; integridad y disponibilidad.

2.1.18. Ataque *CAM Table Overflow*

Definición:
Tipo de ataque que se produce cuando un atacante se conecta a uno o varios puertos de un *switch* o conmutador y ejecuta un programa que simula el acceso de miles de direcciones MAC aleatorias en esos puertos, lo que provoca que se sature la capacidad impidiendo que se puedan atender más peticiones de diferentes MAC. Esto inunda el tráfico del resto de puertos permitiendo al atacante espiar una conversación, entre otras acciones.

2.1.19. 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.

2.1.20. 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.

2.1.21. 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.

2.1.22. Ataque diccionario

Definición:
Véase: Ataque de fuerza bruta

2.1.23. Ataque dirigido

Definición:
Tipo de ataque difícil de detectar que se caracteriza por dirigirse contra un objetivo determinado, durante un periodo de tiempo prolongado, con el fin de conseguir el acceso y control persistente en el sistema atacado. Este ataque consta de una primera fase de recopilación de información para posteriormente ser usada para cumplir los objetivos de los atacantes. Para ello, pueden utilizar diferentes técnicas, como es el uso de correos electrónicos especialmente elaborados, medios de comunicación infectados y técnicas de ingeniería social.

2.1.24. Ataque homográfico

Definición:
Tipo de ataque que se caracteriza por usar URL o direcciones web parecidas a las de páginas legítimas, aunque contienen diferencias inapreciables en caracteres similares provenientes de alfabetos diferentes. Para ello, los ciberdelincuentes tienen en cuenta la psicología y el funcionamiento de la mente humana, ya que esta gestiona de igual forma caracteres similares o aparentemente idénticos. Generalmente, esta técnica se utiliza como parte de un ataque de *phishing*.

Sinónimo: Ataque *punycode*

2.1.25. Ataque pasivo

Definición:
Tipo de ataque difícil de detectar que se caracteriza por la interceptación y monitorización de los datos transmitidos en una comunicación, sin que se produzca algún tipo de modificación de la información transmitida. El principal objetivo de este ataque es la captura, lectura o uso de la información interceptada pero sin modificar su contenido. Los ataques pasivos ponen en riesgo el principio de confidencialidad de la información, pudiéndose mitigar este efecto gracias al uso de cifrado de la información.

2.1.26. 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.

2.1.27. Autenticación

Definición:
Acción mediante la cual demostramos a otra persona o sistema que somos quien realmente decimos que somos, mediante un documento, una contraseña, rasgo biológico etc.

Sinónimo: Autentificación

2.1.28. Autenticidad

Definición:
Véase: No repudio

2.1.29. Autentificación o autenticación básica

Definición
Esquema de autenticación basado en la web más simple que funciona mediante el envío del nombre de usuario y contraseña con cada solicitud.

2.1.30. 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.

2.1.31. Autoridad de registro

Definición:
Es la entidad encargada de identificar de manera inequívoca a los usuarios para que, posteriormente, éstos puedan obtener certificados digitales.

Sinónimo: Autoridad Local de Registro

2.1.32. 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.
• Prestadores de servicios electrónicos de confianza.

2.1.33. 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 LOPDGDD (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

«*Business to bussines,* son las **transacciones comerciales entre empresas**, utilizando medios telemáticos como EDI *(Electronic Data Interchange)* o el comercio electrónico»

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. Bastionado

Definición:
Proceso que trata de reducir las vulnerabilidades y agujeros de seguridad presentes en un sistema, creando un entorno lo más seguro posible siguiendo los principios de: mínima superficie de exposición, mínimos privilegios y defensa en profundidad. Entre las acciones que se realizan para alcanzar este propósito destacan la eliminación de recursos, servicios o programas que no se utilizan, baja de usuarios o cambio de las credenciales o configuraciones establecidas por defecto.

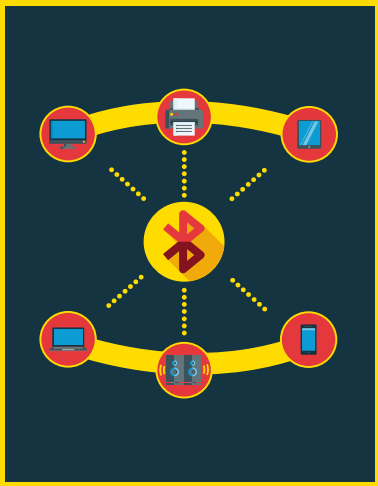
2.2.6. BIA

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.

2.2.7. 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.



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

2.2.8. 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.

2.2.9. 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.

2.2.10. Borrado seguro

Definición:
Método de borrado de archivos que se caracteriza por sobrescribir los datos con el propósito de impedir su recuperación. Esto es aplicable tanto para información en formato físico como digital.

2.2.11. 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.

2.2.12. Bots

Definición:
Ordenador infectado por un troyano que se comunica con un centro de comando y control (*C&C*) para enviarle información robada y recibir actualizaciones. Además, puede realizar otras funciones como enviar *spam*, minar criptomonedas, infectar otros equipos de su red o entorno.

2.2.13. Brecha de seguridad

Definición:
Violaciones de la seguridad que ocasionan la destrucción, pérdida o alteración accidental o deliberada de datos personales cuando están siendo transmitidos, están almacenados o son objeto de otros tratamientos. Las brechas de seguridad también afectan a la comunicación o acceso no autorizados a dichos datos.

2.2.14. 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*

2.2.15. Bulo

Definición:
Mensaje falso muy llamativo con la misión de difusión de mentiras, de visitar una web maliciosa, de recopilar direcciónes de correo, etc. Pueden ser emails, sms, mensajería instantánea etc.

2.2.16. BYOD

Definición:
Acrónimo en inglés de *Bring Your Own Device*; en español, trae tu propio dispositivo. Es una política de uso de la tecnología en las empresas que se caracteriza por permitir a los empleados el uso de sus propios dispositivos personales (portátiles, *smartphones*, tabletas) para el trabajo, así como el acceso desde los mismos a las redes corporativas, aceptando su uso compartido, tanto para las tareas profesionales como para las personales de los empleados.

2.2.17. Bypass

Definición:
Desvío que se utiliza para evitar o solucionar un obstáculo en la comunicación. Podría ser un sistema de seguridad informático o un problema de comunicación, en cuyo caso, el desvío suele ser temporal.

2.3. C

2.3.1. Cadena de custodia

Definición:
Protocolo para la extracción segura y protección de las evidencias digitales, mediante cifrado y sellado de tiempo, para su presentación junto a una demanda o denuncia ante los tribunales o para procesos de auditoría. Abarca en el tiempo todo el proceso; es decir, desde que se realiza el examen del dispositivo, se obtiene la prueba y se expone ante los tribunales o se destruye de forma controlada.

2.3.2. Captcha

Definición:
Acrónimo en inglés de *Completely Automated Public Turing test to tell Computers and Humans Apart*; en español, prueba de *Turing* completamente automática y pública para diferenciar ordenadores de humanos, es un tipo de medida de seguridad que consiste en la realización de pruebas desafío-respuesta controladas por máquinas que sirven para determinar cuándo el usuario es un humano o un *bot* según la respuesta a dicho desafío.

2.3.3. 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

2.3.4. 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.

2.3.5. CERT

Definición:
Acrónimo en inglés de *Computer Emergency Response Team*; en español, equipo de respuesta ante emergencias informáticas, es el equipo de expertos responsables de la respuesta ante incidencias de seguridad que se producen en redes de comunicaciones y sistemas informáticos. Su labor consiste en el desarrollo de medidas preventivas y reactivas que ofrecen como respuesta ante incidentes, como pueden ser la publicación de alertas ante amenazas y vulnerabilidades u ofreciendo ayuda para mejorar la seguridad de un sistema.

2.3.6. 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.

2.3.7. 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.

2.3.8. 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.

2.3.9. Ciberataque

Definición:
Intento deliberado de un ciberdelincuente de obtener acceso a un sistema informático sin autorización sirviéndose de diferentes técnicas y vulnerabilidades para la realización de actividades con fines maliciosos, como el robo de información, extorsión del propietario o simplemente daños al sistema.

2.3.10. Ciberdelincuente

Definición:
Persona que realiza actividades delictivas en la red contra personas o sistemas informáticos, pudiendo provocar daños económicos o reputacionales mediante robo, filtrado de información, deterioro de *software* o *hardware*, fraude y extorsión. Casi siempre están orientados a la obtención de fines económicos.

2.3.11. Ciberejercicio

Definición:
Actividades orientadas a la evaluación del estado de preparación de un individuo, equipo, empresa, sector o país, frente a posibles crisis de origen cibernético que mejoren la respuesta, cooperación y coordinación del personal involucrado.

2.3.12. Cifrado

Definición:
Proceso de codificación de información para poder evitar que esta llegue a personas no autorizadas. Solo quien posea la clave podrá acceder al contenido.

Véase: Algoritmos de cifrado

2.3.13. Cifrado asimétrico

Definición:
También llamado cifrado de clave pública, consiste en una serie de instrucciones mediante funciones matemáticas, que utilizan dos claves que modifican un mensaje digital, haciéndolo ilegible para que solo pueda ser leído por quien posea las dos claves. Dichas claves son: una pública, que puede ser conocida por cualquiera, y otra privada, que solo conocerá el receptor. Cada emisor y receptor tiene su propia parejas de claves unica: una pública y otra privada. Cuando se envía un mensaje, el emisor lo cifra con la clave pública del receptor, quien lo descifrará con su propia clave privada, la cual debe ser mantenida a salvo para asegurar la legitimidad del mensaje. En este tipo de cifrado también se puede verificar si el emisor firma el mensaje con su clave privada, que la identidad de los interlocutores es legítima, suponiendo una comunicación totalmente segura.

Sinónimo: Criptografía asimétrica

2.3.14. Cifrado de extremo a extremo

Definición:
Es la propiedad de algunos sistemas de comunicación que hace que los mensajes intercambiados sean ilegibles durante la comunicación en caso de interceptación al estar cifrados. Al ser de extremo a extremo, implica que solo emisor y receptor podrán descifrar y conocer el contenido del mensaje.

2.3.15. Cifrado simétrico

Definición:
Conjunto de pasos predefinidos y ordenados, consistentes en tratamientos con funciones de cifrado matemático que utilizan claves, para modificar la información en formato digital de un mensaje entre dos interlocutores hasta hacerlo ilegible. El objetivo es evitar que terceras partes, que no dispongan de la clave, puedan conocer la información del mensaje si este es interceptado. Cuando el algoritmo es simétrico las dos partes conocen la clave de cifrado y esta es la misma clave necesaria para el descifrado. Por este motivo, también se conocen como sistemas de secreto o clave compartida.

Sinónimo: Criptografía simétrica

2.3.16. Clave privada

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.

2.3.17. 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.

«***Cloud Computing* o computación en la nube** se refiere a un paradigma que permite ofrecer servicios de computación a través de una red, que normalmente es Internet»

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.

2.3.18. 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

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

2.3.20. Confidencialidad

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

2.3.21. Contraseña

Definición:
Forma de autentificación de un usuario, a través de una clave secreta, para controlar el acceso a algún recurso o herramienta. En caso de que no se proporcione la clave correcta no se permitirá el acceso a dichos elementos.

2.3.22. Contraseña de un solo uso

Definición:
También conocido como OTP (del inglés *One-Time Password*) es una contraseña válida para un solo uso. Puede ser generada por un dispositivo o aplicación en el momento de su utilización. Puede ser utilizada en combinación con otras formas de autenticación: huella digital, contraseña, PIN, tarjeta de coordenadas, etc.

2.3.23. Contraseña débil

Definición:
Tipo de contraseña que se caracteriza por ser corta y haber sido generada por defecto o mediante el uso de nombres propios, variaciones del nombre del usuario o fechas significativas. Son contraseñas que pueden adivinarse de forma rápida mediante el uso de diccionarios.

2.3.24. Contraseña predeterminada

Definición:
Son aquellas contraseñas que vienen asignadas por el fabricante de un dispositivo o *software* de forma masiva, de tal manera que todos los aparatos fabricados tienen la misma y figura en los manuales de puesta en marcha. Esto se considera una vulnerabilidad, aprovechada por los ciberdelincuentes a menudo para acceder a los dispositivos sin autorización. La recomendación es cambiar siempre las contraseñas por defecto.

2.3.25. Contraseña robusta

Definición:
Tipo de contraseña que se caracteriza por ser suficientemente larga, que se crea al azar o mediante la combinación de caracteres alfanuméricos (letras mayúsculas y minúsculas, números y caracteres especiales) que dificultan de forma clara su revelación, ya que se requiere un tiempo elevado de cálculo para lograrlo.

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

2.3.26. Control de acceso

Definición:
Sistema de verificación que permite el acceso a un determinado recurso si la persona o entidad tiene los derechos necesarios para solicitarlo. Este acceso puede ser a recursos de tipo físico (por ejemplo, a un edificio o un departamento) o lógicos (por ejemplo, a un sistema o una aplicación *software* específica).

2.3.27. Control de acceso por roles

Definición:
Sistema de verificación que permite o deniega el acceso a un recurso tecnológico según los derechos concedidos a cada usuario dependiendo de la clase o grupo a la que esté adscrito. Se pueden establecer roles, por ejemplo, por áreas de la empresa (ventas, operaciones...) o por la posición jerárquica dentro de la estructura; cada rol con los permisos necesarios para realizar su trabajo. Al dar de alta a un usuario en el sistema, el admistrador le asignará un rol dependiendo de las tareas que deba realizar y que tendrá asociados los permisos de acceso necesarios.

2.3.28. 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

2.3.29. 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.

2.3.30. Copia de seguridad

Definición:
Proceso mediante el cual se duplica la información existente de un soporte a otro, con el fin de poder recuperar los datos contenidos en caso de fallo del primer soporte de alojamiento.

2.3.31. Correo de suplantación

Definición:
Mensaje de correo electrónico, en teoría legítimo, que usa el nombre de una persona u organismo de confianza con el objetivo de obtener información confidencial o personal de la persona u organización a la que se ha enviado.

2.3.32. Correo *spam*

Definición:
Tipo de correo electrónico que se caracteriza por ser no solicitado por el receptor y que se envía en grandes cantidades con fines publicitarios o como complemento de actividades maliciosas como los ataques de *phishing*.

Sinónimo: Correo basura

2.3.33. 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*

«Es una **moneda digital descentralizada** que no requiere la supervisión de un banco central u organismo regulador para enviar o recibir dinero entre usuarios sin necesidad de intermediarios como por ejemplo *Bitcoin*»

2.3.34. Cracker

Definición:
Ciberdelincuente que se caracteriza por acceder de forma no autorizada a sistemas informáticos con la finalidad de menoscabar la integridad, la disponibilidad y el acceso a la información disponible en un sitio web o en un dispositivo electrónico.

2.3.35. Credenciales

Definición:
Conjunto de datos, generalmente nombre de usuario y contraseña, pudiendo ser también un certificado de usuario, tarjeta inteligente o un token, entre otros. Estos datos posibilitan, por un lado, uno la identificación del individuo como usuario del sistema, y por otro, la autenticación o verificacion de la identidad del individuo para obtener acceso a recursos localizados en equipos locales y en red.

2.3.36. 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.

2.3.37. Criptomoneda

Definición:
Moneda digital descentralizada que no requiere la supervisión de un banco central u organismo regulador para enviar o recibir dinero entre usuarios sin necesidad de intermediarios como por ejemplo *Bitcoin*. Utiliza un esquema P2P (*peer-to-peer*) y tecnologia *blockchain* o de cadena de bloques para generar la cadena de confianza de los registros de las transacciones.

2.3.38. Criticidad

Definición:
Atributo que mide el riesgo que provoca un comportamiento erróneo o negligente respecto a las condiciones normales de funcionamiento al que está sometido un proceso, sistema o equipo. A mayor nivel de criticidad, mayor gravedad de los hechos ocurridos.

2.3.39. 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.

2.3.40. CSIRT

Definición:
Acrónimo de *Computer Security Incident Response Team*, también conocido en español como equipo de respuesta a incidentes de seguridad informáticos, es el equipo encargado de recibir, comprobar y responder a incidentes que se detecten en su área de actuación. Es considerado como el equivalente en Europa de su contraparte estadounidense CERT.

Sinónimo: CERT

2.3.41. CSRF

Definición:
Acrónimo del inglés *Cross Site Request Forgery*; en español, falsificación de petición en sitios cruzados, es un tipo de ataque contra páginas web en el que un *software* malicioso obliga a un sitio web a ejecutar comandos no autorizados en nombre del usuario que accede a dicha página; es decir, explota la confianza que un sitio web tiene en un usuario determinado.

2.3.42. Cuarentena

Definición:
Acción que desarrollan los antivirus para aislar un archivo infectado del resto del sistema. De este modo, se evita que el archivo aislado provoque daños en el sistema hasta que sea posible desinfectarlo con todas las garantías por parte del antivirus. En ocasiones esto no es posible, por lo que se procedería continuando la cuarentena o eliminándolo directamente del sistema.

2.3.43. Cuentas predeterminadas

Definición:
Cuenta establecida por defecto por el sistema o por programa que permite realizar el acceso por primera vez al mismo. Se recomienda que el usuario posteriormente la modifique o la elimine.

2.3.44. CVE

Definición:
Acrónimo del inglés en *Common Vulnerabilities and Exposures*; en español, listado de vulnerabilidades de seguridad conocidas, en el que se puede identificar una vulnerabilidad, así como un resumen de las características, efectos, las versiones del *software* afectadas, posibles soluciones o mitigaciones de dicha vulnerabilidad.

2.3.45. CVSS

Definición:
Acrónimo en inglés de *Common Vulnerability Scoring System*; en español, sistema de puntuación de vulnerabilidad común, es un estándar cuya finalidad es cuantificar la gravedad y estimar el impacto que presentan las vulnerabilidades respecto a la seguridad de un sistema.

2.4. D

2.4.1. Datos personales

Definición:
Información relativa a una persona física viva que puede ser identificada o identificable a través de la recopilación de una serie de datos de carácter personal, que establezcan de forma directa o indirecta un perfil más o menos detallado de su identidad personal, familiar o profesional.

2.4.2. Defacement

Definición:
Tipo de ataque contra un sitio web en el que se modifica la apariencia visual de una página web. Normalmente son producidos por ciberdelincuentes que obtuvieron algún tipo de acceso a la página, bien por algún error de programación de la página, algún *bug* en el propio servidor o una mala administración por parte de los gestores de la web.

2.4.3. Denegación de servicio

Definición:
Ataque a un sistema, aplicación o dispositivo para dejarlo fuera de servicio debido a una saturación de peticiones.

Sinónimo: *Denial Of Service* (Dos)

2.4.4. Denegación de servicio distribuida

Definición:
Es un Dos pero las peticiones se hacen desde diversos orígenes, de esta forma es más efectivo, y más complicado de detener y determinar su origen.

Sinónimo: *Distributted Denial Of Service (DDoS)*

2.4.5. Derecho al olvido

Definición:
Derecho que permite a su titular impedir la difusión de información personal a través de Internet cuando su publicación no cumpla los requisitos de adecuación y pertinencia previstos en la ley, como pueden ser información obsoleta o que no tiene relevancia ni interés público, aunque la publicación original sea legítima.

2.4.6. Desastre natural

Definición:
Tipo de catástrofe que ocasiona pérdidas en bienes materiales o de vidas humanas debido a la acción de eventos o fenómenos naturales, como por ejemplo, terremotos, huracanes, tornados, inundaciones, tsunamis, etc.

2.4.7. 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*

2.4.8. Descifrado

Definición:
Acción de eliminar la codificación de una serie de datos que los convierte en ilegibles, mediante una clave conocida o por medio de técnicas de prueba error. El descifrado convierte el texto oculto por el cifrado en texto claro y legible.

2.4.9. Desmagnetizar

Definición:
Técnica que permite destruir de forma permanente los dispositivos de almacenamiento magnéticos y, por lo tanto, la información que contienen.

2.4.10. Detección de anomalías

Definición:
Medición del comportamiento anómalo de un sistema frente a un perfil de comportamiento normal. Se genera un perfil basado en el comportamiento normal del sistema sin influencias de eventos anómalos o inusuales. A partir de este perfil generado se rastrea por medio del aprendizaje automático el sistema en busca de comportamientos anómalos o maliciosos, como pueden ser intentos de reconocimientos ilegítimos, errores en las conexiones o tráfico de datos inusual en un puerto diferente del preestablecido.

2.4.11. Detección de incidentes

Definición:
Sistema que analiza determinados parámetros y elementos que sirven para monitorizar, detectar y verificar indicios de posibles incidentes de seguridad, que pueden registrarse en el sistema objeto de estudio y evaluación.

«Las direcciones IP son un **número único e irrepetible** con el cual **se identifica a todo sistema** conectado a una red»

2.4.12. 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

2.4.13. 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*

2.4.14. 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.

2.4.15. DLP

Definición:
Acrónimo en inglés de *Data Loss Prevention*; en español, prevención de la pérdida de datos. Los DLP son herramientas que sirven para prevenir las fugas o pérdidas de información originadas dentro de la propia organización, mediante el uso de inteligencia artificial de forma activa que permite monitorizar, detectar y bloquear el acceso a la información según las acciones llevadas a cabo por los usuarios sobre dicha información.

2.4.16. DMZ

Definición:
Acrónimo en inglés de *Demilitarized Zone*; en español, zona desmilitarizada. Consiste en una red aislada que se encuentra dentro de la red interna de la organización. En ella se encuentran ubicados exclusivamente todos los recursos de la empresa que deben ser accesibles desde Internet, como el servidor web o de correo. Por lo general, una DMZ permite las conexiones procedentes tanto de Internet como de la red local de la empresa, donde están los equipos de los trabajadores, pero las conexiones que van desde la DMZ a la red local no están permitidas. Esto se debe a que los servidores que son accesibles desde Internet son más susceptibles a sufrir un ataque que pueda comprometer su seguridad.

2.4.17. 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.

2.4.18. DNS *spoofing*

Definición:
Véase: Envenenamiento del DNS

2.4.19. DNSSEC

Definición:
Acrónimo en inglés de *Domain Name System Security Extensions*; en español, extensiones de seguridad del sistema de nombres de dominio. Consiste en un conjunto de extensiones y especificaciones que añaden una capa de seguridad adicional al protocolo DNS, permitiendo comprobar la integridad y autenticidad de los datos. Gracias a estas extensiones de seguridad se pueden prevenir ataques de suplantación y falsificación.

2.4.20. Doble factor de autenticación

Definición:
Esquema de autenticación básica a la que se añade otro factor como puede ser un código enviado a un móvil, huella dactilar, sistema OTP, etc., más seguro que la autenticación simple.

2.4.21. Downloader

Definición:
Véase: *Dropper*

2.4.22. Dropper

Definición:
Es un fichero ejecutable cuya función es instalar *malware* en el equipo donde se ejecuta. El *malware* puede estar contenido en el programa, aunque lo normal es que lo descargue desde Internet.

2.5. E

2.5.1. e-administración

Definición:
Véase: Administración electrónica

2.5.2. Envenenamiento del DNS

Definición:
Se trata de una actividad maliciosa en la que un ciberatacante trata de obtener el control de un servidor de nombres de dominio de Internet (las máquinas que dirigen el tráfico en la red). En ocasiones se limita tan solo al rúter. Una vez obtenido el control del servidor, las peticiones que le llegan son dirigidas a otros sitios no legítimos colocados por el ciberatacante. Estos sitios están generalmente enfocados a instalar *malware* o realizar actividades ilícitas como *phishings* (suplantaciones de identidad) de otros sitios para obtener un beneficio económico.

«Equipo azul se emplea en ciberseguridad para designar un **equipo humano** encargado de **detener ataques de intrusión en redes y sistemas del ámbito corporativo** por parte de atacantes reales»

2.5.3. Equipo azul

Definición:
Término empleado en ciberseguridad (proveniente del ámbito militar) para designar un equipo humano encargado de detener ataques de intrusión en redes y sistemas del ámbito corporativo por parte de atacantes reales. Su misión es corregir las vulnerabilidades o deficiencias detectadas por un equipo rojo, el cual realiza simulaciones de ataques controlados, así como detener posibles ataques reales. Este tipo de equipos están exclusivamente especializados en monitorizar y reforzar la seguridad de la empresa.

Sinónimo: *Blue Team*

2.5.4. Equipo rojo

Definición:
Término empleado en ciberseguridad (proveniente del ámbito militar) para designar un equipo humano encargado de realizar pruebas de intrusión en redes y sistemas del ámbito corporativo con el fin de evaluar la ciberseguridad de la empresa y detectar vulnerabilidades. Se trata en realidad de una simulación de ataques controlados sin causar daño, en el que las deficiencias detectadas se reportan al equipo azul, encargado de subsanarlas. Su objetivo es detectar las deficiencias antes de que sean explotadas por atacantes reales.

Sinónimo: *Red Team*

2.5.5. Escalada de privilegios

Definición:
Situación que se produce cuando un ciberatacante explota una vulnerabilidad o fallo de una aplicación o sistema, logrando con ello permisos de acceso más amplios de los que inicialmente debería tener. Estos permisos le permiten acceder a ciertas areas reservadas en las que se podría almacenar información sensible susceptible de ser robada.

Sinónimo: Elevación de privilegios

2.5.6. Escaneo de puertos

Definición:
Técnica intrusiva en la que los atacantes buscan de manera activa los puertos y servicios que pudieran estar a la escucha, en busca de recopilar infrormación de la víctima con la finalidad de intentar encontrar vulnerabilidades que explotar en la fase de ataque. Este tipo de técnica también es denominada *fingerprinting*.

2.5.7. Escaneo de vulnerabilidades

Definición:
Actividad en la que se buscan vulnerabilidades en redes y sistemas, mediante diferentes técnicas y aplicaciones especializadas, con el fin de identificarlas y subsanarlas para evitar que sean utilizadas por los ciberdelincuentes en su beneficio. El escaneo se centra en las aplicaciones, puertos y servicios desplegados en una empresa.

2.5.8. Esteganografía

Definición:
Técnica que consiste en ocultar un mensaje dentro de un archivo aparentemente normal denominado portador, como puede ser una imagen, escondiendo su existencia para que no sea detectado.

2.5.9. 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. Falso negativo

Definición:
Error que se produce al realizar un análisis del sistema mediante un *software* antivirus que detecta un archivo libre de virus cuando realmente está infectado.

2.6.2. Falso positivo

Definición:
Error que se produce al realizar un análisis del sistema mediante un *software* antivirus que detecta un archivo como infectado cuando realmente está libre de virus.

2.6.3. Fichero ejecutable

Definición:
Archivo diseñado para inicializar un programa (instalación, ejecución, etc.) debido a que en su interior están las instrucciones precisas para poder ejecutar un *software* determinado.

2.6.4. Filtrado de paquetes

Definición:
Mecanismo de un cortafuegos que permite controlar el acceso a una red interna a través del análisis de tráfico de paquetes tanto entrantes como salientes, teniendo en cuenta una serie de parámetros (dirección IP de origen y de destino, protocolo, etc.), así como su inclusión en una lista negra de IPs.

2.6.5. Fingerprint

Definición:
Véase: Huella digital

2.6.6. Fingerprinting

Definición:
Método de recopilación de información de un dispositivo, persona u organización con el fin de facilitar su identificación. Para lograrlo se usan lenguajes de *scripting* del lado cliente que permiten recopilar información sobre el usuario o dispositivo seleccionado, como pueden ser tipo y versión del navegador y sistema operativo, resolución de la pantalla, *plugins*, micrófono, cámara, etc. Además de recopilar información sobre los hábitos y gustos sin que los usuarios lo sepan, también puede ser utilizado por ciberdelincuentes para descubrir qué módulos de *software* (versión específica del navegador, *plugins*, etc.) instalados en un dispositivo específico y ser vulnerados mediante el uso de *exploits*.

Sinónimo: Reconocimiento, recopilación de información

2.6.7. Firma antivirus

Definición:
Entrada en la base de datos del antivirus, también conocido como diccionario, que sirve como forma de identificación de un tipo de *malware* en concreto.

«La **firma electrónica** se define como el conjunto de datos electrónicos que acompañan o que están asociados a un documento electrónico»

2.6.8. 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

2.6.9. Firmware

Definición:
Tipo de *software* que permite proporcionar un control a bajo nivel de un dispositivo o componente electrónico, siendo capaz de proveer un entorno de operación para las funciones más complejas del componente o comportándose como sistema operativo interno en armonía con otros dispositivos o componentes.

2.6.10. Footprint

Definición:
Término empleado en ciberseguridad para referirse a la recolección de información de un sistema, susceptible de ser empleada en un ciberataque. Dicha información se suele encontrar disponible generalmente en canales de acceso público, como buscadores de Internet. El *footprint* es el rastro dejado por el concepto que se pretende investigar y que define en mayor o menor medida un sistema, red o empresa.

«La fuga de datos es la **pérdida de la confidencialidad de la información privada** de una persona o empresa»

2.6.11. Fraude del CEO

Definición:
Ataque de ingeniería social, variante del *spear phishing*, que se caracteriza porque el fraude está dirigido a miembros concretos de la organización, principalmente ejecutivos de alto nivel, con el objeto de obtener sus claves, contraseñas y todo tipo de información confidencial que permita a los atacantes el acceso y control de los sistemas de información de la empresa. La forma en que se comete el ataque bajo esta figura es muy similar a la de los ataques de *phishing*. Se procede mediante el envío de correos electrónicos falsos que contienen enlaces a sitios web fraudulentos, con la diferencia de que en el caso de *phishing* el afectado no es necesariamente un directivo o alto cargo de la organización.

Sinónimo: *Whaling*

2.6.12. 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.

2.6.13. 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

2.6.14. Fuga de información

Definición:
Proceso por el cual se produce una fuga de la información almacenada en una red interna o en dispositivos físicos provocada por un atacante malintencionado y que es volcada o publicada en Internet para su libre consulta por parte de terceros sin autorización.

«El gestor de contraseñas permite tener diferentes contraseñas por cada sitio para **incrementar así la seguridad**»

2.7. G

2.7.1. Gestión de incidentes

Definición:
Listado de procedimientos previamente documentados sobre los pasos a seguir en caso de detectar una amenaza de ciberseguridad en la empresa. La gestión de incidentes está orientada a mitigar en el menor tiempo posible un incidente de seguridad identificándolo y asignando el personal que dará respuesta al mismo dentro de unos parámetros predefinidos.

2.7.2. Gestor de contraseñas

Definición:
Programa o aplicación que se puede integrar en los principales navegadores y que permite generar contraseñas robustas y almacenarlas cifradas junto con los nombres de usuario para diferentes sitios web y aplicaciones, con la facilidad de tener que recordar solo la contraseña de acceso al gestor. Esto permite tener diferentes contraseñas por cada sitio para incrementar así la seguridad. Algunos de ellos ofrecen además servicios adicionales, como el autocompletado de datos personales, servicios en la nube y autenticación de doble factor para acceder a las contraseñas almacenadas.

2.7.3. GNU *Privacy Guard*

Definición:
Implementación completa y gratuita del estándar *OpenPGP* que permite cifrar y firmar los datos y comunicaciones a través de un sistema de gestión de claves versátil, junto con módulos de acceso para todo tipo de directorios de claves públicas. Gracias a esta versatilidad es posible su uso e integración en otras aplicaciones.

2.7.4. 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.

«Persona con grandes conocimientos en el manejo de las tecnologías de la información que **investiga un sistema informático** para reportar fallos de seguridad y desarrollar técnicas que previenen accesos no autorizados»

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. Hacker

Definición:
Persona con grandes conocimientos en el manejo de las tecnologías de la información que investiga un sistema informático para reportar fallos de seguridad y desarrollar técnicas que previenen accesos no autorizados.

2.8.2. Hacktivista

Definición:
Ciberdelincuente que haciendo uso de sus conocimientos en materia informática y herramientas digitales los usa para promover su ideología política. Entre las acciones que realizan destacan las modificaciones de webs (*defacement*), redirecciones, ataques de denegación de servicio (DoS), robo de información privilegiada o parodias de sitios web, entre otras. Estos actos son llevados a cabo por estas personas bajo la premisa de potenciar otros actos como la desobediencia civil con el fin último de lograr sus propósitos políticos.

2.8.3. Hardening

Definición:
Véase: Bastionado

2.8.4. Hash

Definición:
Operación criptográfica que genera identificadores alfanuméricos, únicos e irrepetibles a partir de los datos introducidos inicialmente en la función. Los *hashes* son una pieza clave para certificar la autenticidad de los datos, almacenar de forma segura contraseñas o firmar documentos electrónicos, entre otras acciones.

Sinónimo: Función resumen

«HTTP son las siglas en inglés de Protocolo de Transferencia de Hipertexto. **Se trata del protocolo más utilizado para la navegación web**»

2.8.5. Heartbleed

Definición:
Vulnerabilidad descubierta que afecta a la librería OpenSSL y que compromete la información protegida por los métodos de cifrado SSL/TLS al permitir que cualquiera que esté observando el tráfico (conexiones VPN, servicios HTTPS o servicios de correo) entre sistemas protegidos por la versión de OpenSSL afectada, pueda leer el contenido de la información transmitida, al estar comprometidas las claves de seguridad secretas que se usan para cifrar el tráfico de los usuarios, los nombres de usuarios, las contraseñas y el contenido que se transmite.

2.8.6. Hoax

Definición:
véase: Bulo

2.8.7. Honeypot

Definición:
Herramienta de seguridad instalada en una red o sistema informático que permite, ante un ataque informático por parte de terceros, poder detectarlo y obtener información tanto del ataque como del atacante.

Sinónimo: Señuelo

2.8.8. 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.

2.8.9. 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.

2.8.10. Huella digital

Definición:
Mecanismo cuyo propósito principal es combatir la piratería digital y defender los derechos de autor mediante la introducción de una serie de bits o datos aleatorios imperceptibles que permiten detectar si la copia es legítima o no.

2.9. I

2.9.1. ICMP *Tunneling*

Definición:
Un túnel ICMP funciona inyectando datos arbitrarios en un paquete de eco enviado a un dispositivo remoto. La respuesta sigue el mismo patrón, inyectando una respuesta en otro paquete ICMP y enviándola de regreso. La tunelización ICMP se puede utilizar para evitar las reglas de los *firewalls* mediante la ofuscación del tráfico real para llevar a cabo diferentes tipos de ataque como fugas de información.

2.9.2. Identificación

Definición:
Acción mediante la cual le decimos a otra persona o sistema quiénes somos.

2.9.3. 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.

2.9.4. Impacto

Definición:
Medida del efecto que produce un incidente, desastre, problema o cambio en los niveles de servicio de una empresa y cómo se ven afectados en el caso de que se materialice dicha amenaza.

2.9.5. 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.

2.9.6. Indicadores de compromiso

Definición:
Los indicadores de compromiso o *Indicators of Compromise* (IOCs) hacen referencia a una tecnología estandarizada que consiste en definir las características técnicas de una amenaza por medio de las evidencias existentes en un equipo comprometido; es decir, se identifican diferentes acciones como ficheros creados, entradas de registro modificadas, procesos o servicios nuevos, etc.; de manera que puedan servir para identificar otros ordenadores afectados por la misma amenaza o prevenirlos de la misma.

Sinónimo: IOC

2.9.7. Información sensible

Definición:
Nombre que recibe la información privada y que debe protegerse del acceso de personas no autorizadas sin importar el soporte en el que se encuentre o transmita.

2.9.8. 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.

Sinónimo: Análisis forense digital

2.9.9. Infraestructura crítica

Definición:
Activos de carácter esencial e indispensable cuyo funcionamiento es imprescindible y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales. La proteccion de estas infraestructuras se rige en base a una serie de medidas establecidas por la "Ley 8/2011, de 28 de abril"

2.9.10. 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

2.9.11. Ingeniería inversa

Definición:
Proceso mediante el cual se obtiene la información o el diseño de un producto con el propósito de determinar el proceso de fabricación o creación de sus componentes y de qué manera interactúan entre sí hasta lograr el producto final. Aplicado al *software*, la ingeniería inversa es la actividad que se ocupa de descubrir cómo funciona un programa, función o característica, de cuyo código fuente no se dispone, hasta generar código propio que cumpla las mismas funciones.

Sinónimo: Desensamblaje

2.9.12. Ingeniería social

Definición:
Conjunto de técnicas que los delincuentes usan para engañar a los usuarios de sistemas/servicios TIC para que les faciliten datos que les aporten valor, ya sean credenciales, información sobre los sistemas, servicios instalados etc.

2.9.13. Insider

Definición:
Persona perteneciente a una organización o empresa que divulga información sensible sobre dicha empresa de forma intencionada.

2.9.14. 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.

2.9.15. Intranet

Definición:
Red de comunicación interna de una organización que usa la tecnología del protocolo de Internet para compartir información, dispositivos o *software*.

2.9.16. Intrusión

Definición:
Acción provocada por un atacante o usuario malintencionado, que se aprovecha de una vulnerabilidad en el sistema para conseguir acceder a un área o dispositivo sin autorización con el objetivo de realizar actividades ilegítimas.

2.9.17. Inundación ICMP

Definición:
Ataque de denegación de servicio que consiste en enviar de forma continua un gran número de paquetes ICMP de gran tamaño, provocando una sobrecarga en la red en la que se encuentra el objetivo del ataque al no poder procesar correctamente el servidor todas las peticiones que recibe.

2.9.18. Inundación IP

Definición:
Ataque de denegación de servicio que consiste en enviar de forma continua un elevado número de paquetes IP, provocando la saturación y bloqueo del equipo sistema objetivo del ataque.

2.9.19. Inyección de código

Definición:
Proceso mediante el cual se introduce en un determinado *software* una serie de instrucciones que no formaban parte de la composición original del código de dicho programa o aplicación, pudiendo provocar comportamientos anómalos para los que no fue diseñado en el origen.

2.9.20. 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*

2.9.21. IoT

Definición:
Abreviación del término en inglés *Internet of Things*; en español, Internet de las cosas, es un concepto que se refiere a la interconexión digital de objetos cotidianos, como relojes, cámaras de grabación, electrodomésticos, etc. mediante Internet.

2.9.22. IPS

Definición:
Siglas de *Intrusion Prevention System* (sistema de prevención de intrusiones). 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.

2.9.23. IPsec

Definición:
Conjunto de protocolos cuyo propósito principal es asegurar las comunicaciones que se realizan a través del Protocolo de Internet (IP) autenticando y/o cifrando cada paquete IP que se envía o recibe.

2.10. J

2.10.1. Jailbreak

Definición:
Se trata del proceso con el que conseguimos eliminar las limitaciones de seguridad impuestas por Apple en un dispositivo con iOS. Una vez "liberado", podemos, por ejemplo, instalar aplicaciones de terceros que no estén en AppStore.

«*Keylogger* es un **tipo de *spyware*** que se encarga de **monitorizar toda la actividad realizada con el teclado** para luego enviarla al ciberdelincuente»

2.11. K

2.11.1. Kerberos

Definición:
Protocolo de autenticación de red creado por el Instituto Protocolo de autenticación de red creado por el Instituto Tecnológico de Massachusetts (MIT), diseñado para proveer una autenticación fuerte para las aplicaciones cliente/servidor mediante el uso de la criptografía de clave secreta.

2.11.2. Keylogger

Definición:
Es un tipo de *spyware* que se encarga de monitorizar toda la actividad realizada con el teclado (teclas que se pulsan) para luego enviarla al ciberdelincuente.

2.12. L

2.12.1. 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

2.12.2. LDAP

Definición:
Protocolo a nivel de aplicación que permite el acceso centralizado, una vez se ha autenticado el usuario a través de sus credenciales, a un servicio de directorio ordenado y distribuido que contiene información sobre el entorno de red.

«El *login* es un **mecanismo de acceso a un sistema o servicio** a través de la identificación mediante **credenciales de usuario**»

2.12.3. Lista blanca

Definición:
Lista de direcciones IP o de correo electrónico a los que se pueden enviar mensajes o correos a cuentas del dominio, evitando que sean etiquetadas como *spam* o correo basura.

Sinónimo: Lista de permitidos

2.12.4. Lista negra

Definición:
Lista de direcciones IP o de correo electrónico a los que se bloquea el envío de mensajes a cuentas del dominio, siendo etiquetados como correo basura o *spam* y enviados a la papelera.

Sinónimo: Lista de bloqueados

2.12.5. Log

Definición:
Registros de eventos de la actividad de los usuarios y de los procesos asociados a dicha actividad, como pueden ser el inicio/salida de sesión, tiempo de actividad o conexiones, entre otros. Esta información ayuda a detectar fallos de rendimiento, mal funcionamiento, errores e intrusiones que permiten generar alertas en tiempo real gracias a los datos proporcionados a los sistemas de monitorización.

2.12.6. Login

Definición:
Mecanismo de acceso a un sistema o servicio a través de la identificación mediante credenciales del usuario.

2.12.7. LOPDGDD

Definición:
Acrónimo de Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales, ley española en la que se transpone el reglamento europeo de Protección de datos o RGPD, mediante la cual se regula el tratamiento de los datos de carácter personal, garantizando a los usuarios un mayor control sobre el uso que se hace de los datos por parte de empresas u organismos oficiales, entre otros.

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

2.12.8. LSSI-CE

Definición:
Acrónimo de Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico, ley que regula en España los aspectos jurídicos de las actividades de comercio electrónico, contratación en línea, información y publicidad y servicios de intermediación, y que debe cumplir una empresa o persona desde el momento en el que la actividad en Internet reporte cualquier tipo de beneficio económico o lucrativo al prestador del servicio, ya sea a través de una página web, tienda en línea o *blog*.

2.13. M

2.13.1. Malvertising

Definición:
Véase: *Adware*

2.13.2. 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

2.13.3. MAM

Definición:
Acrónimo en inglés de *Mobile Application Management*; en español, gestión de aplicaciones móviles. Consiste en una implementación del *software* y los servicios responsables de proveer y controlar el acceso a aplicaciones móviles desarrolladas en entornos empresariales, tanto en los dispositivos corporativos como en los personales, siguiendo la filosofía BYOD. Esta implementación proporciona controles a nivel de aplicación que permiten a los administradores gestionar y proteger los datos de la aplicación, así como controlar el dispositivo mediante la instalación de un agente de servicio.

2.13.4. Man-in-the-Middle

Definición:
Se produce cuando una comunicación es espiada entre el emisor y el receptor del mensaje. En algunos casos la información se modifica mediante la inyección de paquetes con algún fin malicioso.

Sinónimo: Hombre en medio

2.13.5. MDM

Definición:
Acrónimo en inglés de *Mobile Device Management*; en español, gestión de dispositivos móviles, consiste en la implementación que permite administrar de forma combinada y escalable, teniendo en cuenta las políticas corporativas e infraestructura de la organización, las aplicaciones y configuraciones de los dispositivos de los empleados, con el propósito de aumentar la compatibilidad, la seguridad y la funcionalidad corporativa de los dispositivos usados en la infraestructura, simplificando su gestión por parte de los administradores de la misma.

2.13.6. Medio de propagación

Definición:
Vías de entrada en los sistemas digitales (puertos, correo electrónico, unidades extraíbles, etc.) a través de las cuales se transmite una infección o se propaga un ataque.

2.13.7. 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.

2.13.8. Mínimo privilegio

Definición:
Estrategia de seguridad basada en la idea de conceder únicamente aquellos permisos estrictamente necesarios para el desempeño de una determinada actividad.

2.13.9. Mitigación

Definición:
Reducción o atenuación de los daños potenciales sobre los sistemas, aplicaciones y dispositivos causados por un evento, como una vulnerablidad o ataque.

2.14. N

2.14.1. NGFW

Definición:
Término proveniente del inglés *New Generation Firewall*, es un cortafuegos de nueva generación, llamado así por estar formado por diferentes elementos, cada uno de los cuales ofrecerá una característica distinta, lo que permite una mejor capacidad de procesamiento, y ante la caída de uno de los servicios, el resto puede seguir funcionando con normalidad. Por el contrario, la adquisición de estos dispositivos y sus respetivas licencias conlleva un coste más elevado que la obtención de un UTM.

2.14.2. 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

2.15. O

2.15.1. Ofuscar

Definición:
Acción o acto deliberado para ocultar o encubrir el mensaje de una comunicación o el código de una aplicación mediante un cambio no destructivo que provoca que sea confusa y complicada de interpretar. De esta forma, se dificulta o impide la aplicación de ingeniería inversa.

2.15.2. OTP (*One-Time Password*)

Definición:
Véase: Contraseña de un sólo uso

2.16. P

2.16.1. 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

2.16.2. Packet injection

Definición:
Acción mediante la cual alguien intercepta una comunicación, capturando paquetes de información e introduciendo en la comunicación otros nuevos manipulados por el atacante con fines maliciosos.

Sinónimo: Inyección de paquetes

2.16.3. 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 seguridad 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

2.16.4. Pasarela de pago

Definición:
Servicio de pago e intermediación que permite a las tiendas online realizar operaciones de pago con los clientes mediante el intercambio de datos, de forma segura y rápida, entre la entidad bancaria del vendedor y la del comprador.

2.16.5. 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.

2.16.6. 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

2.16.7. 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.

«El *phishing* es un **tipo de ataque** en el que alguien suplanta a una entidad/ servicio mediante un correo electrónico o mensaje instantáneo para **conseguir las credenciales o información de la tarjeta de crédito de un usuario**»

2.16.8. 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.

2.16.9. Phishing

Definición:
Técnica o tipo de ataque en el que alguien suplanta a una entidad/servicio mediante un correo electrónico o mensaje instantáneo para conseguir las credenciales o información de la tarjeta de crédito de un usuario. Ese correo/mensaje suele tener un enlace (o fichero que contiene ese enlace) a un sitio web que suplanta al legítimo y que usan para engañarlo.

Sinónimo: *Vishing, Smishing*

2.16.10. PIN

Definición:
Acrónimo del inglés *Personal Identification Number*; en español, número de identificación personal. Tipo de contraseña, generalmente de cuatro dígitos, usada en determinados dispositivos y servicios para identificarse y obtener acceso al sistema.

2.16.11. Ping

Definición:
Utilidad de diagnóstico que mide el estado, velocidad y calidad de una red de comunicaciones mediante el envío de paquetes de solicitud y de respuesta a uno o varios dispositivos.

2.16.12. Ping flood

Definición:
Saturación de una línea de comunicación provocada por el número excesivo de paquetes ICMP en circulación que produce la degradación de otros servicios o protocolos en funcionamiento debido al incremento de los tiempos de respuesta.

2.16.13. 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.

2.16.14. 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

2.16.15. Plan director de seguridad

Definición:
Proyecto consistente en la definición y priorización de un conjunto de medidas en materia de seguridad de la información, con el objetivo de reducir los riesgos a los que está expuesta la organización hasta unos niveles aceptables, a partir de un análisis de la situación inicial. Es fundamental para la realización de un buen plan director de seguridad que se alinee con los objetivos estratégicos de la empresa, incluyendo una definición del alcance e incorporando las obligaciones y buenas prácticas de seguridad que deberán cumplir los trabajadores de la organización, así como terceros que colaboren con esta.

2.16.16. Plugin

Definición:
También conocida como extensión, complemento o *add-on* es una aplicación que se relaciona con otra para agregarle una función nueva y generalmente muy específica. Las extensiones son un tipo de software que permite personalizar entre otros los navegadores web.

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

2.16.17. 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.

2.16.18. Privacidad

Definición:
Derecho de las personas y usuarios a proteger sus datos en Internet, además de controlar el acceso a los mismos y decidir qué información es visible para el resto de actores.

2.16.19. 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.

2.16.20. 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

2.16.21. 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.

Al 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*

2.16.22. Puerta de enlace

Definición:
Dispositivo que actúa como intermediario permitiendo conectar redes con protocolos y arquitecturas diferentes a todos los niveles de comunicación y compartir recursos entre varios dispositivos. Su propósito es traducir la información del protocolo utilizado en una red al protocolo usado en la red de destino. Como característica adicional, el dispositivo que ejerce como puerta de enlace cuenta como mínimo con 2 tarjetas de red. Es importante que el tráfico de datos que atraviesa estas puertas de enlace que intercomunican redes, este supervisado o filtrado para evitar posibles ciberataques.

Sinónimo: *Gateway*

2.16.23. 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.

Sinónimo: *Backdoor*

2.16.24. Puerto

Definición:
Es una interfaz o «puerta» a través de la cual se pueden enviar y recibir datos. Existen dos tipos de puertos: los físicos, que serían los conectores de un equipo que permiten la comunicación entre dispositivos, y que a su vez se dividen en varios tipos según el conector y su función; y los lógicos, generalmente implementados por *software*, que son aquellos que permiten la comunicación entre dos máquinas en una red, mediante áreas de memoria reservadas en un sistema. Los puertos lógicos están limitados a 65536 al tratarse de numeros de 16 bits, que son manejados por las máquinas para establecer las comunicaciones. Los puertos son el principal objetivo de un ciberatacante para identificar posibles vías de entrada a un sistema.

2.17. R

2.17.1. Ransomware

Definición:
Malware cuya funcionalidad es «secuestrar» un dispositivo (en sus inicios) o la información que contiene de forma que si la víctima no paga el rescate, no podrá acceder a ella.

2.17.2. Rat

Definición:
Acrónimo en inglés de *Remote Administration Tool o Remote Administration Trojan*; en español, herramienta o troyano da administración remota, es el programa o *software* usado para la administración remota de un sistema a través de una red, ya sea de forma legítima o no con o sin autorización del usuario del equipo. Su uso es habitual entre los ciberdelincuentes para controlar una máquina infectada mediante una puerta trasera o *backdoor*.

2.17.3. 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

«**RFID**, siglas de ***Radio Frequency Identification***, en español, Identificación por Radiofrecuencia, es un **método de identificación de dispositivos por ondas de radio**»

2.17.4. Redundancia

Definición:
Propiedad consistente en un determinado fichero o sistema para que en caso de caída de uno se pueda seguir proporcionando el servicio.

2.17.5. Repudio

Definición:
Denegación realizada por una de las partes intervinientes en una comunicación, por lo que no se puede garantizar la fuente de la información o de los datos.

2.17.6. Resiliencia

Definición:
Capacidad de una organización de resisitir ante una situación adversa, como por ejemplo, un incidente de ciberseguridad. La resiliencia empresarial debería ir acompañada de un plan de contingencia y continuidad para hacer frente a posibles situaciones de crisis en la empresa.

2.17.7. Respuesta de incidentes

Definición:
Se trata de un plan o guía con el que poder dar respuesta a posibles incidentes de ciberseguridad en la empresa. Dicha guía debe contemplar varios puntos esenciales, detección y registro del incidente, análisis y evaluación, notificación y equipo o personal encargado de su resolución, así como soluciones y mejoras para evitar futuras incidencias. Todo ello siempre atendiendo a la ley RGPD en materia de protección de datos.

2.17.8. 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.

2.17.9. RGPD

Definición:
Acrónimo de Reglamento General de Protección de Datos, regulación de la Unión Europea introducida en 2016 orientada a la protección de los datos personales de las personas físicas por parte de organizaciones e instituciones que operan en la Unión Europea, así como de los procesos que estas realizan de dicha información personal (procesamiento, almacenamiento o destrucción) y las consecuencias y multas en caso de sufrir una filtración o pérdida de información personal por parte de las organizaciones.

2.17.10. Riesgo

Definición:
Es la posibilidad de que una amenaza o vulnerabilidad se convierta en un daño real para la empresa, que resulte en una pérdida o robo de información o en una detención de su actividad como consecuencia del daño ocasionado. El riesgo puede ser mitigado mediante políticas de seguridad y continuidad del negocio que suelen prever posibles ataques y proponen soluciones de actuación ante situaciones cuyo riesgo pueda ser elevado.

2.17.11. Rogue Access Point

Definición:
Punto de acceso inalámbrico que ha sido instalado en una red segura por parte de un ciberdelincuente con el objetivo de suplantar la identidad del acceso legítimo y poder robar información confidencial.

2.17.12. Rootear Android

Definición:
Mediante este proceso se obtiene acceso *root* al dispositivo; es decir, obtener permisos de "superusuario" o administrador, con los que se tendrá acceso al sistema sin ningún tipo de restricción impuesta por el fabricante.

2.17.13. Rootkit

Definición:
Tipo de *malware* que permite un acceso continuo con permisos de administrador a un determinado dispositivo, como un ordenador, y que mantiene su presencia oculta al control de los administradores.

2.17.14. 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

2.17.15. 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.

2.18. S

2.18.1. 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.

2.18.2. Sandbox

Definición:
Se define como un entorno de pruebas aislado que permite ejecutar aplicaciones peligrosas o dudosas sin riesgo de poner en peligro otros sistemas de la organización empresarial. Los *sandboxes* también tienen la función contraria: ejecutar un programa en un entorno seguro, libre de virus y ataques externos. Por ejemplo, si abrimos un archivo adjunto de correo que contiene *malware*, la infección solo afectará al sistema que ejecuta *sandbox*, generalmente, sistemas temporales que una vez cerrados no dejan ninguna secuela por posibles infecciones.

2.18.3. Scam

Definición:
En español, estafa, utilizado para referirse a las estafas por medios electrónicos, bien sea a través de campañas de correo, ofreciendo productos o servicios falsos, o mediante sitios web que venden supuestos productos o servicios inexistentes. El *scam* suele hacer uso de la ingeniería social para engañar a sus víctimas.

2.18.4. Scareware

Definición:
Se trata de un tipo de estafa mediante técnicas de ingeniería social, en la que aparecen ventanas emergentes de forma repetitiva de un supuesto *software* legítimo, generalmente antivirus o *antimalware*, que trata de hacer creer al usuario que su equipo es víctima de una seria amenaza, ofreciéndole al mismo tiempo una solución inminente y rápida a su problema por un módico precio. Su objetivo en muchos casos es triple: si el usuario cae en la trampa estará adquiriendo un *software* falso que no cumple con su fin; por otro lado, los atacantes habrán obtenido sus datos bancarios; y finalmente, el *software* descargado les permitirá acceder al dispositivo de la víctima.

2.18.5. Segmentación de red

Definición:
Técnica que consiste en dividir una red informática en otras redes más pequeñas o segmentos. El objetivo es aumentar el rendimiento de la red mejorando el ancho de banda al reducir el número de integrantes que se comunican entre sí. También se mejora la seguridad de la misma, permitiendo el acceso a determinados segmentos y solo al personal autorizado. De esta forma, en caso de un ciberataque a una red, solo se compromete el segmento afectado y no toda la red corporativa. Actualmente, algunas de las tecnologías más extendidas son las listas ACL (de control de acceso) y las VLAN (redes de area local virtuales).

2.18.6. Seguridad por oscuridad

Definición:
Se trata de un concepto que pretende emplear el secreto de implementación de un dispositivo o programa; es decir, encubrir cómo está construido interiormente para evitar sufrir ataques o vulnerabilidades y tratar de aumentar así el nivel de seguridad. Sin embargo, esta técnica ha sido ampliamente discutida, demostrando que no es efectiva y que incluso es contraproducente, ya que pueden existir vulnerabilidades solo conocidas por unos pocos que permitirían romper la seguridad de lo que se pretende encubrir.

2.18.7. Sello de confianza

Definición:
Son distintivos que garantizan la seguridad, calidad y transparencia de una actividad comercial en Internet, así como las buenas prácticas que se implementan para desarrollarla. Existen diversas organizaciones que emiten estos distintivos previa solicitud y posterior auditoría, algunos ejemplos representativos son Aenor y Confianza Online.

2.18.8. 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.

2.18.9. Session Hijacking

Definición:
También llamado secuestro de *cookies*, es un ataque basado en interceptar la sesión de un usuario en Internet para acceder a su información o servicios sin autorización. Se suele dar en sesiones no cifradas como las HTTP. Este tipo de ataque se ayuda de varias técnicas como *Man-in-the-Middle* o XSS (*cross site scripting*) para lograr su objetivo, así como de programas de *malware* específicos para robar *cookies* de sesión.

2.18.10. SFTP

Definición:
Es la abreviatura en inglés de *Secure File Transfer Protocol*; en español, protocolo de transferencia segura de archivos. Es un protocolo que permite la transferencia de datos de forma segura entre cliente y servidor haciendo uso de SSH (*Secure Shell*), el cual permite mantener ilegible la identidad del usuario y la información intercambiada mediante algoritmos de cifrado.

2.18.11. 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.

2.18.12. Shadow IT

Definición:
Relativo a la utilización del *hardware* y/o *software* dentro de una empresa que no es aceptado con el Departamento Informático o que es utilizado por los empleados sin conocimiento de dicho departamento. Generalmente, conlleva riesgos para la organización al no estar sujetos a las políticas de seguridad corporativas. Este término suele hacer alusión a aquellos dispostivos BYOD (propios de los empleados) como teléfonos móviles o memorias USB, así como al *software* y servicios en la nube.

2.18.13. SIEM

Definición:
Acrónimo de las siglas en inglés *Security Information and Event Management*; en español, gestión de eventos e información de seguridad. Se trata de un *software* con el que se intenta detectar y prevenir amenazas para atajarlas antes de que ocurran. El término comprende, por un lado, el almacenamiento y análisis de eventos en tiempo real SEM; y por otro, el almacenaje para su posterior análisis SIM. De la unión de los dos nace el SIEM, su objetivo es recopilar, identificar y analizar los eventos de seguridad de forma rápida para prevenir posibles ataques y vulnerabilidades.

2.18.14. 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*.

2.18.15. 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

2.18.16. 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).

2.18.17. 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.

2.18.18. SOC

Definición:
Del inglés *Security Operations Center*; en español, centro de operaciones en seguridad. Se trata de un equipo cualificado específicamente en ciberseguridad

con las herramientas necesarias para poder analizar, investigar y dar soporte convenientemente a posibles eventos de ciberseguridad corporativos. Un SOC puede ser externo o interno, y su objetivo es evitar y mitigar posibles ataques en la empresa, constituyendo lo que podríamos llamar contramedidas ante un ciberataque.

2.18.19. Software

Definición:
Definimos *software* del inglés como un conjunto de programas, instrucciones y reglas informáticas que permiten ejecutar distintas tareas en un dispositivo. El *software* conforma todas aquellas acciones que se pueden realizar gracias a las instrucciones previamente contempladas y programadas e incluidas dentro de un programa que permite al usuario interactuar con el sistema de forma fácil e intuitiva.

2.18.20. Spear phishing

Definición:
Modalidad de *phishing* dirigido contra un usuario u organización en concreto en la que los atacantes intentan mediante un correo electrónico, que aparenta ser de un amigo o de empresa conocida, conseguir información confidencial. Este tipo de ataques suelen contar previamente con una fase de reconocimiento donde los ciberdelincuentes obtienen la información necesaria para perpetrar el ataque.

2.18.21. 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*.

2.18.22. 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

2.18.23. SSID

Definición:
Acrónimo del inglés *Service Set Identifier*; en español, identificador de conjunto de servicios, es una secuencia alfanumérica que permite identificar una red de área local wifi de otras redes inalámbricas de la zona.

2.18.24. 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 inglés de «seguridad de la capa de transporte» (*Transport Layer Security*) protocolo ampliamente utilizado en la actualidad.

Sinónimo: TLS

2.18.25. 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.

2.19. T

2.19.1. Tablas *rainbow*

Definición:
Tablas especialmente diseñadas para encontrar coincidencias de un determinado *hash*, resultado de aplicar la función resumen sobre una contraseña en texto plano. Este tipo de tablas reducen considerablemente el tiempo necesario en realizar ataques de fuerza bruta sobre contraseñas.

2.19.2. 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.

2.19.3. Texto plano

Definición:
Archivo informático que carece de formato y que contiene texto formado por caracteres alfanuméricos legibles por humanos.

2.19.4. Token

Definición:
Dispositivo físico (*hardware*) o digital (*software*) que permite el acceso a un recurso restringido en lugar de usar una contraseña, firma digital o dato biométrico; es decir, actúa como una llave con la que acceder a un recurso.

2.19.5. Troyano

Definición:
Malware diseñado para tener múltiples utilidades, la más común es crear una puerta trasera en el equipo infectado, para poder descargar actualizaciones y nuevas funcionalidades. Esta diseñado para ser controlado desde un centro de comando y control (C&C). Como funcionalidades habituales encontramos: *keylogger*, escaneo de redes locales buscando otros equipos para infectar, envío de correos, robo de datos/ficheros, minado de cryptomonedas, descarga de otros *malwares* como *ransomware*... La distribución suele hacerse usando un correo electrónico con un fichero adjunto o enlace a un fichero, que es quien prepara el equipo para descargar el troyano e infectarlo. La mayor parte del *malware* actual son Troyanos, más del 80%. Los ordenadores infectados con un troyano se denominan *Bots* o Zombi, y un grupo de *bot* controlados por un C&C se denomina *Botnet* o Red Zombie.

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

2.19.6. Túnel

Definición:
Técnica que encapsula un protocolo de red sobre otro, lo que permite generar un túnel de comunicación para transportarlo a través de una red con seguridad. Destaca el uso de esta técnica en redes privadas virtuales o VPN.

2.20. U

2.20.1. 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.

2.20.2. UTM

Definición:
Acrónimo en inglés de *Unified Threat Management*; en español, gestión unificada de amenazas, es el *software* de seguridad perimetral que permite la gestión centralizada de las amenazas que pueden afectar a una organización. Para ello, se ubica la misma en un punto intermedio de la red interna para inspeccionar la información en tránsito desde y hacia Internet.

2.21. V

2.21.1. 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.

2.21.2. Virus

Definición:
Malware que tiene como característica principal que infecta ficheros ejecutables o sectores de arranque de dispositivos de almacenamiento

2.21.3. 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*.

2.21.4. 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.

2.21.5. VPN

Definición:
Véase: Red Privada Virtual

2.21.6. Vulnerabilidad

Definición:
Debilidad o fallo de un sistema que puede ser aprovechado con fines maliciosos (normalmente mediante un programa que se denomina *exploit*). Cuando se descubre el desarrollador del *software* o *hardware* lo solucionará publicando una actualización de seguridad del producto.

Sinónimo: Agujero de seguridad

«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»

2.22. W

2.22.1. Watering hole

Definición:
Se produce cuando el atacante infecta una página legítima, que es visitada regularmente por las víctimas a quien se dirige la acción, para que esos visitantes queden infectados al visitarla.

Sinónimo: Abrevadero

2.22.2. WEP

Definición:
Acrónimo en inglés de *Wired Equivalent Privacy*; en español, privacidad equivalente a cableado, es el sistema de cifrado que permite proteger la información que se transmite a través de redes wifi. Actualmente, se considera un protocolo débil y se desaconseja su uso.

2.22.3. 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.

Preferiblemente se deben utilizar como sistemas de cifrado:

- WPA2
- WPA3

Sinónimo: Wi-Fi, WiFi

2.22.4. Wi-Fi Direct

Definición:
Estándar de las conexiones inalámbricas wifi que permite establecer de forma directa la conexión entre dos dispositivos sin un punto de acceso inalámbrico intermedio; es decir, a través de un solo salto.

2.22.5. WPA

Definición:
Acrónimo en inglés de *Wi-Fi Protected Access*; en español, acceso protegido inalámbrico, consiste en un sistema usado en el ámbito de las comunicaciones inalámbricas destinado a evitar que cualquier persona no expresamente autorizada pueda acceder a la red mediante el uso de este algoritmo de cifrado. Ha sido desarrollado por la *Wi-Fi Alliance* como alternativa al algoritmo WEP y, actualmente, se encuentra implementada la versión 3 de dicho algoritmo (WPA3).

2.22.6. WPS

Definición:
Del inglés *Wifi Protected Setup*, es un mecanismo creado para facilitar la conexión de dispositivos a una red Wi-Fi. Debido a un fallo de seguridad presente en el mecanismo, un atacante podría acceder de manera muy facil a la red, por lo que se recomienda desactivarlo. Tras este fallo se desarrolló el mecanismo *Wi-Fi Direct*.

2.23. X

2.23.1. 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

2.24. Z

2.24.1. 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*

2.24.2. 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*

2.25. 0-9

2.25.1. 0-day

Definición:
Véase: Zero-day

2.25.2. 2FA

Definición:
Véase: Doble factor de autenticación

3. Fuentes de referencia

[REF - 1] Panda. Glosario.
http://www.pandasecurity.com/spain/homeusers/security-info/glossary

[REF - 2] NICCS. Cybersecurity Glossary.
https://niccs.us-cert.gov/about-niccs/cybersecurity-glossary

[REF - 3] NIST. Glossary.
https://csrc.nist.gov/glossary/term/US_CERT

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA SEGUNDA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD
017
protege tu empresa