Uruguay Presidencia | agesic

Glosario de términos de ciberseguridad

Autor / Seguridad de la Información

Versión: 2

Año 2023

Glosario de términos de ciberseguridad

Resumen

Este glosario recoge los términos de seguridad que aparecen en las publicaciones y materiales de las campañas de Seguro Te Conectás.

Para la definición de los términos se han utilizado las fuentes de referencia, las definiciones del Marco de Ciberseguridad de Agesic y otros documentos propios, como guías e informes. La finalidad es permitirles a las personas una mayor comprensión de la ciberseguridad, profundizando en determinados términos o conceptos y evitando precisiones por demás técnicas.

A

Activo de información

Son aquellos datos o informaciones que tienen valor para la empresa. Pueden ser procesos de negocios, datos, aplicaciones, equipos informáticos, personal, soportes de información, redes, equipamiento auxiliar o instalaciones.

Actualización de seguridad

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.

Adware

Software que rastrea el navegador y el historial de descargas del usuario con la intención de mostrar anuncios emergentes o banners no deseados para atraerlo a realizar una compra o hacer clic en un enlace.

Sinónimo: Malvertising

Algoritmos de cifrado

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.

Alta disponibilidad

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.

Amenaza

Causa potencial de un incidente no deseado que puede dar lugar a daños en un sistema o en una organización. Una amenaza puede ser natural, accidental o intencionada.

Análisis de riesgos

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.

Análisis de vulnerabilidades

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.

Antispyware

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.

Antivirus

Es un tipo de software cuyo objetivo es detectar, bloquear y eliminar malware, término que refiere a un software malicioso, del inglés malicious software.

Sinónimo: Antimalware

Aplicación

Es un programa informático diseñado como herramienta para permitir a un usuario realizar uno o diversos tipos de tareas en un dispositivo.

Sinónimo: Software

Ataque de fuerza bruta

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.

Autenticación

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.

B

Banner

Es una pieza publicitaria que aparece dentro de una página web. En casi todos los casos, su objetivo es atraer tráfico hacia el sitio web del anunciante, que paga por su inclusión.

Blog

Un blog es un sitio web que incluye, a modo de diario personal de su autor, contenidos de su interés, que suelen estar actualizados con frecuencia y a menudo son comentados por los lectores.

Botnet

Una botnet es un conjunto de computadoras (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.

Bots

Computadora infectada 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.

Brecha de seguridad

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.

Sinónimo: Vulnerabilidad de seguridad

Bug

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

Sinónimo: Error de software

Buscador

Es un sistema informático que busca páginas o archivos almacenados en servidores web. Las búsquedas se hacen con palabras clave o con árboles jerárquicos por temas; el resultado de la búsqueda es un listado de direcciones web en las que se mencionan temas relacionados con las palabras clave buscadas.

C

Cadena de custodia

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.

Captcha

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 computadoras 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.

Ciberataque

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.

Ciberdelincuente

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.

Cifrado

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

Confidencialidad

Es la propiedad de la información que determina que esta no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

Junto con la integridad y la disponibilidad suponen las tres dimensiones de la seguridad de la información.

Contraseña

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.

Contraseña débil

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.

Contraseña predeterminada

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.

Contraseña segura

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.

Sinónimo: Contraseña robusta

Control de acceso

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).

Control de acceso por roles

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.

Control parental

Conjunto de herramientas o medidas que se pueden tomar para evitar que los menores de edad hagan un uso indebido de la computadora y 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 una computadora 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 de este, que normalmente deberá ser el padre o tutor del menor.

Sinónimo: Control paterno

Cookie

Una cookie es un pequeño archivo 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 un ataque contra la privacidad de los usuarios y es por lo que hay que tener cuidado con ellas.

Copia de seguridad

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.

Correo de suplantación

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.

Credenciales

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 verificación de la identidad del individuo para obtener acceso a recursos localizados en equipos locales y en red.

Criptografía

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.

Criticidad

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.

Cuarentena

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.

Cuentas predeterminadas

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.

CVE

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.

CVSS

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.

D

Datos personales

Información de cualquier tipo referida a personas físicas o jurídicas determinadas o determinables (artículo 4 de la Ley N° 18.331). Son datos personales, entre otros, el

nombre, el apellido, el correo electrónico, el celular, una fotografía, la huella dactilar, el modelo retinal, la voz, la imagen de una persona, el RUT y el ADN.

Datos sensibles

Datos personales que revelen origen racial y étnico, preferencias políticas, convicciones religiosas o morales, afiliación sindical e informaciones referentes a la salud o a la vida sexual (artículo 4 de la Ley N° 18.331). Estos datos tienen una protección especial por parte de la ley.

Defacement

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.

Denegación de servicio

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

Sinónimo: Denial Of Service (Dos)

Dinero electrónico

Es una forma de representar el dinero en efectivo, por ejemplo, mediante tarjetas pre pagas, billeteras electrónicas o instrumentos similares emitidos por instituciones emisoras de dinero electrónico o empresas de inter mediación financiera. Funciona como una tarjeta de débito, con la diferencia de que no está asociado a una cuenta bancaria. Es aceptado como medio de pago, convertible en dinero en efectivo, no genera intereses y su valor se almacena en medios electrónicos, como chips, discos duros o servidores.

Dirección IP

Las direcciones IP (del inglés IP: Internet Pro tocol) son un número único e irrepetible con el cual se identifica a todo sistema conectado a una red. Podríamos compararlo con la matrícula de un vehículo.

Sinónimo: IP

Dirección MAC

Acrónimo del inglés Media Access Control, traducido al español como Control de Acceso al Medio, 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.

Sinónimo: dirección física, dirección hardware

Disponibilidad

Propiedad de la información que determina que la misma sea accesible y utilizable por solicitud de una persona, entidad o servicio autorizado cuando este lo requiera.

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

Doble factor de autenticación

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.

Sinónimo: 2FA, Autenticación de dos factores

E

Escaneo de vulnerabilidades

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.

Estafa nigeriana

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: Carta nigeriana, Cuento del tío.

Evento de seguridad

Hecho que indica una posible brecha de ciberseguridad o falla de controles.

Exploit

Secuencia de comandos o herramientas utilizadas 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 por ejemplo: 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

F

Firmware

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.

Firewall

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: Cortafuegos

Fuga de datos

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

Fuga de información

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.

G

Gestión de incidentes

Es un proceso que tiene como principal objetivo tener un enfoque estructurado y bien planificado que permita tratar adecuadamente los incidentes de ciberseguridad, asistiendo a los involucrados, de forma de reducir el impacto de los incidentes.

Gestión de vulnerabilidades

Es el proceso mediante el cual se identifican las vulnerabilidades, se identifican los sistemas afectados y se toma acción para reducir los riesgos de que las amenazas puedan utilizar estas vulnerabilidades y ocasionar un incidente.

Gestor de contraseñas

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.

Gusano

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 archivo infectado, los gusanos realizan copias de sí mismos, infectan a otras computadoras y se propagan automáticamente en una red independientemente de la acción humana.

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

Sinónimo: Worm

H

Hacker

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.

Hash

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.

Host

Un host es cualquier dispositivo de hardware (computadora u otro dispositivo) que tiene la capacidad de permitir el acceso a una red a través de una interfaz de usuario, software especializado, dirección de red, o cualquier otro medio.

Sinónimo: anfitrión

HTTP

Son las siglas del inglés Hypertext Transfer Protocol. Es un protocolo de transferencia donde se utiliza un sistema que permite el intercambio de información y procesamiento de servicios que ofrecen las páginas web.

HTTPS

A diferencia del tráfico “http”, el “https” es el uso de un algoritmo de cifrado simétrico cuya clave ha sido previamente intercambiada entre el navegador y el servidor. Al igual que “http”, se usa para la trasferencia de datos, pero de forma segura.

Huella digital

La huella digital en internet refiere al conjunto único de actividades, acciones, contribuciones y comunicaciones digitales rastreables, que se manifiestan en Internet o en dispositivos digitales.

Sinónimo: Sombra digital.

I

Identificación

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

Impacto

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.

Incidente de seguridad informática

Es una violación o una amenaza inminente de violación a una política de seguridad de la información implícita o explícita, así como un hecho que compromete la seguridad de un sistema: confidencialidad, integridad o disponibilidad (artículo 3 del Decreto N° 451/009 de 28 de setiembre 2009).

Sinónimo: incidente de ciberseguridad

Infección

Es la acción que realiza el malware al ingresar a cualquier dispositivo electrónico (PC, tableta, celular, etc.).

Información sensible

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.

Ingeniería social

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.

Integridad

Es la propiedad de la información por la que 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.

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

Intrusión

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.

IoT

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.

L

LAN

Una LAN (del inglés Local Area Network) es una red informática de pequeña amplitud geográfica, que suele limitarse a espacios como una oficina, una vivienda o un edificio.

Una LAN permite interconectar distintos dispositivos todo tipo, computadoras, 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 dispositivos.

Sinónimo: Red de Área Local

LDAP

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.

Link

Es un elemento de un documento electrónico que permite acceder directamente a otro documento o a otra parte de este, o a un sitio web.

Sinónimo: Enlace, Vínculo

Lista blanca

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

Lista negra

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

Log

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.

Sinónimo: Registro

Login

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

M

Malware

Del inglés malicious software, término que engloba a todo tipo de programa o código malicioso cuya función es dañar un sistema o causar un mal funcionamiento. Dentro de este grupo podemos encontrar: virus, troyanos, gusanos, keyloggers, botnets, ransomwares, spyware, adware, rootkits y bootkits, entre otros.

Sinónimo: Software malicioso

Menor privilegio

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

Sinónimo: Mínimo privilegio

Mitigación

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

N

Navegador

Es un software, aplicación o programa que permite el acceso a la web, interpretando la información de distintos tipos de archivos y sitios web para que estos puedan ser visualizados.

No repudio

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 Sinónimo: Autenticidad

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, archivos y datos en servidores de terceros, de forma que puedan ser accesibles desde cualquier dispositivo con acceso a la nube, resultando de esta manera innecesaria la instalación de software adicional en el dispositivo usuario.

Sinónimo: Cloud computing, computación en la nube, cloud

P

P2P

P2P (del inglés Peer-to- Peer) es un modelo de comunicaciones entre sistemas 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 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

Parche de seguridad

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

Pasarela de pago

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.

Pentest

Una prueba de penetración es un ataque a un sistema de software o hardware con el objetivo de encontrar vulnerabilidades que tiene un alcance definido. 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 potencial atacante 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, Ethical hacking

Phishing

Conjunto de técnicas que persiguen el engaño de una persona, imitando la identidad de un tercero de confianza, como podría ser un banco, una institución pública, empresa o red social, con el fin de manipularla y lograr que realice acciones que no debería (por ejemplo, revelar información confidencial, hacer clic en un enlace a una página fraudulenta brindando información personal como el usuario o la contraseña, o descargar archivos infectados con malware).

Variantes de la técnica: Vishing, Smishing

PIN

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.

R

Ransomware

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.

Red social

Plataformas informáticas diseñadas para albergar comunidades virtuales de individuos interconectados que comparten contenido, información, archivos, fotos, audios, videos, etc.

Respaldo de la información

Copia de seguridad que se realiza sobre archivos o aplicaciones contenidas en una computadora, dispositivo o aplicación con la finalidad de recuperar los datos en 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 respaldo pueden ser discos duros, USB o DVD. También es común la realización de copias de seguridad mediante servicios de copia basados en la nube.

Sinónimo: Copia de seguridad, Copia de respaldo, Respaldo, Backup.

Riesgo

Potencial que una amenaza dada explote vulnerabilidades de un activo o grupo de activos, ocasionando un daño.

Router

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

S

Scam

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.

Seguridad informática

Conjunto de medidas preventivas y reactivas que tienen como objetivo mantener la confidencialidad, disponibilidad e integridad de la información soportada en medios informáticos.

Servidor

Puede entenderse como servidor tanto el software que realiza ciertas tareas en nombre de los usuarios, como la computadora física en la 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.

Sistemas automatizados de evaluación de vulnerabilidades (VAS)

Son herramientas que permiten identificar las vulnerabilidades en los sistemas.

Sinónimo: VAS

SLA

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 SLA 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

Software

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.

Sinónimo: Programa, aplicación

SPAM

Mensaje basura o spam refiere a aquellos mensajes no deseados, que pueden llegar de remitentes conocidos, o no conocidos e incluso falsos.

Normalmente tienen un objetivo publicitario, y suelen ser enviados de forma masiva y pueden verse en varios tipos de comunicación: llamadas telefónicas, SMS, correos electrónicos, etc.

Sinónimo: Correo basura, Correo electrónico no deseado.

Spyware

Es un tipo de malware que espía el dispositivo afectado. Sus funciones son recoger datos e información del dispositivo y observar la actividad del usuario sin su consentimiento.

Sinónimo: Programa espía.

SSL

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

Suplantación de identidad

Es la actividad maliciosa en la que un atacante se hace pasar por otra persona para cometer algún tipo de fraude.

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

T

Texto plano

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

Token

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.

Troyano

Es un tipo de malware que accede al sistema como un archivo o aplicación inofensiva y realiza acciones no deseadas en segundo plano.

U

URL

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.

V

Virus

Es un tipo de malware que tiene como característica principal que infecta archivos ejecutables o sectores de arranque de dispositivos de almacenamiento.

Busca modificar el funcionamiento normal del dispositivo. Requiere la interacción de una persona para propagarse a otros archivos y sistemas.

VPN

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: Red privada virtual

Vulnerabilidad de seguridad

Es un fallo técnico o deficiencia de un sistema que puede afectar la disponibilidad, integridad o confidencialidad de la información pudiendo llevar a cabo operaciones no permitidas de manera remota.

Sinónimo: Agujero de seguridad, Brecha de seguridad

Fuentes de referencia

- INCIBE. Glosario.
- NICCS. Cybersecurity Glossary.
- NIST. Glossary.