

SEGURIDAD INFORMÁTICA



[Mis cursos](#) > [23-38/002065](#) > [MF0490_3 Gestión de servicios en el sistema informático](#) > [Actividad 01. Elaboración de glosario de términos](#)

[Imprimir](#)


jueves, 11 de julio de 2024, 08:49

Sitio: **Centro de Estudios Master**Curso: **SEGURIDAD INFORMÁTICA (23-38/002065)**Glosario: **Actividad 01. Elaboración de glosario de términos****A**

Actividad 01 René Verstraete

Buenos días,

Adjunto actividad de glosario de términos en PDF

 [Actividad 01 Glosario de términos René Verstraete.pdf](#)

Actividad 01. Glosario de términos

Buenos días,

Adjunto actividad de glosario de términos.

 [Actividad 01 Glosario de términos.docx](#)

Actividad 1 Glosario

Glosario terminos seguridad informatica

 [ACTIVIDAD 1.docx](#)

Acuerdo de licencia

Los acuerdos de licencia son **contratos legales vinculantes que definen las relaciones de licencia de contenidos entre propietarios de contenidos (licenciantes) y distribuidores de contenidos (licenciarios).**

Administración Electrónica

Se basa en el uso de las tecnologías de la información y la comunicación (TIC) para diseñar, desarrollar e implantar herramientas y entornos informáticos que permitan la comunicación, las gestiones y los trámites de la ciudadanía y las empresas con la administración.

Adware (Malvertising)

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

AES (Advanced Encryption Standard)

Algoritmo de cifrado simétrico utilizado para asegurar datos electrónicos. Es reconocido por su alta velocidad y seguridad y es ampliamente usado en aplicaciones de software y hardware para proteger información confidencial.

Alta disponibilidad

Hace referencia a la disponibilidad ininterrumpida de los recursos del sistema del equipo. En un dominio de Informática, la alta disponibilidad elimina un único punto de posibles errores y minimiza la interrupción del servicio en caso de error.

Amenaza

Circunstancia desfavorable que puede ocurrir y que cuando sucede tiene consecuencias negativas sobre los activos provocando que no se encuentre disponible, 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.

Análisis de malware

Proceso de estudiar el comportamiento y características de un **malware** para comprender su funcionamiento, origen y objetivos. Esto incluye identificar el tipo de malware, sus vectores de infección¹, sus mecanismos de propagación² y sus efectos³ en los sistemas afectados.

(1) vectores de infección: Métodos o vías a través de los cuales un malware o una amenaza cibernética puede ingresar a un sistema o red: correos electrónicos de phishing, descargas de archivos infectados, vulnerabilidades en software, unidades USB comprometidas, sitios web maliciosos, etc

(2) mecanismos de propagación: Métodos que usa el malware para pasar de unos sistemas a otros: Correos electrónicos de phishing, Descargas drive-by, Compartición de archivos en redes P2P, Dispositivos USB infectados, Vulnerabilidades de software, Redes sociales, Publicidad maliciosa (malvertising), Aplicaciones móviles infectadas, Explotación de contraseñas débiles, Redes Wi-Fi no seguras, etc.

(3) efectos del malware: Pérdida de datos, ralentización del sistema, robo de información personal, daño a la reputación, pérdidas financieras, interrupción del servicio, vulnerabilidades de seguridad adicionales, secuestro de datos, revelación de información o secretos, etc

Antispyware

Software diseñado para detectar y eliminar programas espía (spyware) que recopilan información sobre una persona o empresa sin su conocimiento, afectando la privacidad y seguridad del usuario.

Ataque activo

Un ataque activo es un tipo de ataque cibernético en el que un intruso intenta alterar o comprometer la integridad, confidencialidad o disponibilidad de un sistema informático o red, en lugar de simplemente observar o recopilar información.

Ataque CAM Table Overflow

Tipo de ataque cibernético dirigido a switches de red (conmutadores) que tienen como objetivo saturar la tabla de direcciones MAC (Content Addressable Memory) del switch. Se dirige específicamente a la infraestructura de red de una empresa, con el objetivo de desestabilizar y comprometer la seguridad de la red interna.

Ataque combinado

Es un tipo de ataque cibernético que utiliza varios métodos o vectores diferentes para comprometer la seguridad de un sistema o red.

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.

Ataque de fuerza bruta

Un ataque de fuerza bruta es un método de piratería informática que utiliza pruebas y errores para descifrar contraseñas, credenciales de inicio de sesión y claves de cifrado.

Ataque dirigido

Un ataque dirigido es una forma de ciberataque planificado y dirigido contra una entidad específica con el objetivo de infiltrarse en sistemas de información para robar datos, espiar, o causar daños.

Ataque homográfico

Un ataque homográfico es una técnica utilizada por los ciberdelincuentes para engañar a los usuarios y obtener información confidencial, como contraseñas o datos de tarjetas de crédito

Auditoría de seguridad

Evaluación sistemática y exhaustiva de los sistemas y prácticas de seguridad de una organización para identificar vulnerabilidades y garantizar el cumplimiento de políticas de seguridad.

Autenticación

En ciberseguridad, la autenticación es el proceso de verificar la identidad de alguien o algo. La autenticación suele tener lugar mediante la comprobación de una contraseña, un token de hardware o algún otro dato que demuestre la identidad.

Autenticación multifactor (MFA)

Método de autenticación que requiere dos o más formas de verificación para conceder acceso a un recurso.

Por ejemplo, una contraseña combinada con un código enviado al teléfono móvil del usuario o una huella dactilar, proporcionando una capa adicional de seguridad.

Autoridad de certificación

Una autoridad de certificación (CA) es una entidad que valida la identidad digital de sitios web, direcciones de correo electrónico, empresas o personas individuales. Para ello, utilizan activos criptográficos denominados certificados digitales, que proporcionan una forma de demostrar la autenticidad

Aviso Legal

Un aviso legal o descargo de responsabilidad es una referencia a las notificaciones que se encuentran comúnmente en e-mensajes de correo electrónico y páginas web, que establece los derechos del lector de un documento en particular y la responsabilidad del usuario y del autor.

B

B2B (Business-to-Business)

Tipo de transacción comercial entre empresas, en la que un negocio vende productos o servicios a otro negocio. Estas transacciones suelen ser de mayor volumen y valor en comparación con las transacciones entre empresas y consumidores (B2C).

Backup

Copia de seguridad de los datos realizada en un soporte de almacenamiento adecuado (un disco duro externo, por ejemplo). Al hacer un backup, se crea una copia de seguridad de los datos a partir de la cual se pueden restaurar posteriormente en caso de pérdida.

BIA

Análisis de impacto en el negocio (Business Impact Analysis) es una fase del Plan de Continuidad de Negocio con el que debe contar cualquier empresa u organización. Permite identificar con claridad los procesos misionales de cada entidad y analizar el nivel de impacto con relación a la gestión del negocio.

Biometria

Haciendo referencia a las tecnologías de la información, la biometría hace referencia a métodos de identificación mediante técnicas matemáticas y estadísticas sobre rasgos físicos o de conducta para poder verificar la identidad de un individuo

Blockchain

Tecnología de base de datos distribuida que asegura la **integridad** y la **transparencia** de las transacciones mediante el uso de criptografía y consenso descentralizado¹. Cada bloque contiene una lista de transacciones, y una vez que se añade al blockchain, es casi imposible de modificar sin alterar todos los bloques posteriores, lo que garantiza la inmutabilidad y la seguridad de los datos.

(1)consenso descentralizado: proceso mediante el cual múltiples nodos o participantes distribuidos en la red llegan a un acuerdo sobre el estado y la validez de las transacciones sin depender de una autoridad central

Bomba lógica

Tipo de malware que se activa cuando se cumplen ciertas condiciones predefinidas, como una fecha específica o una acción del usuario. Una vez activada, la bomba lógica puede realizar acciones destructivas, como borrar datos o dañar el sistema.

Borrado seguro

Método para eliminar datos de un dispositivo de almacenamiento de forma que sea imposible recuperarlos. Esto se logra sobrescribiendo los datos originales con patrones de datos aleatorios o usando técnicas específicas de destrucción de datos.

Bot

Programa informático que a través de una cadena de comandos o funciones autómatas previas efectúan automáticamente tareas mediante internet

Botnet

Botnet es un término que hace referencia a un conjunto o red de robots informáticos o bots, que se ejecutan de manera autónoma y automática.¹ El artifice de la botnet puede controlar todos los ordenadores/servidores infectados de forma remota.

En los sistemas Windows y macOS la forma más habitual de expansión de los "bots" suele ser en la distribución de software ilícito, pese a que se puede expandir mediante cualquier software sospechoso. Este tipo de software suele contener malware el cual, una vez el programa se ejecuta, puede escanear su red de área local, disco duro, puede intentar propagarse usando vulnerabilidades conocidas de Windows, etc.

C

Captcha

CAPTCHA (prueba de Turing completamente automática y pública para diferenciar ordenadores de humanos) es una prueba desafío-respuesta controlada por máquinas (no es necesario ningún tipo de mantenimiento ni de intervención humano en su realización, ya que es implementado en un ordenador) que son utilizadas para determinar cuándo el usuario es un humano o un programa automático (bot).

Cartas nigerianas

Tipo de estafa también conocida como "estafa 419", en la cual los estafadores prometen una gran suma de dinero a cambio de un pequeño adelanto por parte de la víctima, que nunca se recupera.

Centro de respaldo

Ubicación física o virtual utilizada para almacenar copias de seguridad de datos y sistemas críticos de una organización. Estos centros permiten la recuperación de información en caso de desastres, fallos de hardware o ciberataques.

CERT

Un CERT (Computer Emergency Response Team) es un equipo de personas dedicado a prevenir, detectar y responder eficazmente a los incidentes de seguridad que puedan materializarse sobre los sistemas informáticos. Su objetivo es limitar el daño en estos sistemas y garantizar la continuidad de los servicios que soportan

Certificado digital

Un Certificado Electrónico (o certificado digital) es un fichero digital emitido por una tercera parte de confianza (una Autoridad de Certificación) que garantiza la vinculación entre la identidad de una persona o entidad y su clave pública

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.

Cifrado simétrico

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

Clave privada

Es la encargada de descifrar la información en la criptografía asimétrica, propia de los certificados digitales. La clave privada es generada por la Autoridad de Certificación a la hora de emitir un certificado y solo es conocida por el usuario que se identifica como titular del mismo.

Clave pública

Es un método para encriptar o firmar datos con dos claves diferentes y hacer que una de las claves, la pública, esté disponible para que cualquiera pueda utilizarla.

Códigos de conducta

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.

Compromiso de cuentas

Situación en la que se accede a una cuenta de usuario de forma no autorizada. Esto puede resultar en el robo de información personal, el uso indebido de recursos, la suplantación de identidad y otros actos maliciosos. El compromiso o situación de cuenta comprometida puede ocurrir debido a:

- Contraseñas débiles (ataques de fuerza bruta, por diccionario, etc)
- Phishing
- Troyanos (espionaje por keylogger)
- Vulnerabilidades de software
- Redes inalámbricas no securizadas
- Sitios web fraudulentos
- Reutilización de contraseñas
- Engaños mediante ingeniería social
- Acceso físico a dispositivos de protección o equipos informáticos

Contraseña predeterminada

Una contraseña predeterminada es una contraseña comúnmente conocida y establecida por el fabricante de un dispositivo o software, que se utiliza para acceder al mismo en el primer inicio o en casos de restauración de fábrica. Estas contraseñas suelen ser fáciles de adivinar y pueden ser utilizadas por atacantes para acceder a los sistemas o dispositivos de los usuarios.

Control de acceso

Conjunto de métodos y tecnologías utilizados para regular quién o qué puede ver o usar recursos en un entorno de computación, asegurando que solo los usuarios autorizados tengan acceso.

Control parental

Conjunto de herramientas y configuraciones disponibles en dispositivos y servicios digitales que permiten a los padres monitorear y restringir el acceso de sus hijos a contenido inapropiado o peligroso, gestionar el tiempo de uso y supervisar la actividad en línea

Cookie

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 capturando para cada página que navega.
- 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.

Correo de suplantación (Pishing)

Técnica fraudulenta en la que se envían correos electrónicos que parecen provenir de fuentes confiables con el objetivo de engañar a los destinatarios para que revelen información personal, como contraseñas, números de tarjetas de crédito u otra información sensible.

Correo spam

Correo electrónico comercial no solicitado (UCE), consiste en anuncios no deseados y cuestionables enviados por correo electrónico de forma masiva.

Cracker

Persona que intenta acceder a un sistema informático sin autorización. El término identifica a individuos malintencionados que actúan con un único objetivo: violar la seguridad de un sistema cibernético de forma ilegal. A diferencia de los hackers, sus fines son casi siempre malintencionados, se valen de sus conocimientos técnicos exclusivamente para invadir sistemas, descifrar claves y contraseñas, robar datos y demás usos digitales ilícitos. Su modus operandi se basa en explotar las vulnerabilidades de programas y sistemas informáticos, asaltando información privada para hacer un uso personal y malintencionado de ella.

Criptografía

Disciplina matemática e informática relacionada con la seguridad de la información, particularmente con el cifrado y la autenticación. En cuanto a la seguridad de aplicaciones y redes, es una herramienta para el control de acceso, la confidencialidad de la información y la integridad.

Criptografía de Curva Elíptica (ECC)

Tipo de criptografía basada en estructuras algebraicas de curvas elípticas. La ECC proporciona niveles muy altos de seguridad con claves más pequeñas y eficientes en comparación con otros métodos criptográficos como RSA, lo que permite operaciones más rápidas y menor consumo de recursos en dispositivos limitados.

Criticidad

Los análisis de criticidad de activos son un instrumento que permiten establecer jerarquía o prioridades de procesos, sistemas y equipos, creando una estructura que facilita la toma de decisiones acertadas para lograr una mejor priorización de los programas y planes de mantenimiento.

CRL

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.

CSRF

Cross Site Request Forgery (CSRF o XSRF) es un tipo de ataque que se suele usar para estafas por Internet. Los delincuentes se apoderan de una sesión autorizada por el usuario (session riding) para realizar actos dañinos. El proceso se lleva a cabo mediante solicitudes HTTP.

Cuarentena

Zona de almacenamiento especial que contiene copias de seguridad de archivos que se han eliminado o modificado durante la desinfección. La función principal de Cuarentena es permitir al usuario restaurar un archivo original en cualquier momento.

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

(Common Vulnerabilities and Exposures), es un sistema de catalogación pública que identifica y enumera las vulnerabilidades de seguridad conocidas en productos software y hardware que está desarrollado y mantenido por el MITRE con el respaldo de la comunidad de ciberseguridad.

CVSS

Sistema común de puntuación de vulnerabilidades. Se trata de un proceso de evaluación que otorga un resultado confiable y objetivo para conocer con exactitud en qué nivel de vulnerabilidad se encuentra un sistema informático.

D

Datos personales

Cualquier información que puede ser utilizada para identificar a una persona, como nombre, dirección, número de teléfono, dirección de correo electrónico, número de identificación, datos biométricos, etc.

Deepfake

Tecnología que utiliza inteligencia artificial para crear imágenes, audio o videos falsos pero altamente realistas. Esta técnica puede superponer la cara o cuerpo de una persona sobre otra en un video, haciendo que parezca que está diciendo o haciendo algo que en realidad no hizo; también puede simular la voz de una persona a partir de pequeñas muestras de audio, lo que plantea serias preocupaciones de seguridad y ética, ya que puede crear suplantaciones de personas altamente creíbles

Denegación de servicio (DoS - Denial of Service)

Tipo de ataque cibernético que busca hacer que un servicio, sistema o red se vuelva inaccesible para sus usuarios legítimos mediante la sobrecarga del recurso con tráfico excesivo o explotando vulnerabilidades del sistema.

Denegación de servicio distribuida (DDoS)

Tipo de ataque que busca hacer que un servicio, red o sitio web no esté disponible para los usuarios legítimos, saturando el sistema con una gran cantidad de tráfico desde múltiples fuentes.

Derecho al olvido

El derecho que cualquier persona tiene para solicitar la supresión de sus datos personales en los buscadores de internet, hacer que se borre información sobre ellas después de un período de tiempo determinado.

Desbordamiento de búfer

Anomalía que se produce cuando el software que escribe datos en un búfer desborda la capacidad del búfer, lo que provoca que se sobrescriban las ubicaciones de memoria adyacentes.

Desbordamiento de Buffer

En el ámbito de la seguridad informática, se trata de una técnica consistente aprovechar un fallo en la programación de los servicios o aplicaciones (vulnerabilidad de software) para provocar un comportamiento no esperado de un sistema y que revele cierta información, ejecute comandos o acceda a información de forma no autorizada.

Para ello, el atacante provoca que la cantidad de información enviada al sistema sea muy superior al el volumen de datos donde se tiene que alojar. En el caso de existir vulnerabilidad al no compruebarse la capacidad, se produce un 'desbordamiento' de datos sobrescriben en otros puntos de la memoria, lo cual puede hacer que el programa falle produciendo comportamientos inesperados, e incluso, que permita introducir código malicioso.

Descifrado

El desciframiento es un conjunto de técnicas de análisis de códigos que permite conocer e interpretar toda o parte de la información expresada mediante un código desconocido (es decir, un código cuyas reglas de codificación convencionales son desconocidas).

Desmagnetizar

Técnica de borrado seguro que se utiliza para eliminar permanentemente la información almacenada en medios magnéticos, como discos duros o cintas de respaldo.

Detección de anomalías

La detección de anomalías identifica actividades sospechosas que no entran dentro de los patrones normales establecidos de comportamiento. Una solución protege el sistema en tiempo real frente a instancias que podrían provocar pérdidas financieras significativas, violaciones de datos y otros eventos perjudiciales.

Detección de incidentes

Proceso y conjunto de herramientas y técnicas utilizadas para identificar, analizar y responder a eventos de seguridad que puedan comprometer la integridad, disponibilidad o confidencialidad de la información. La detección de incidentes es crucial para minimizar el impacto de ciberataques y otros eventos de seguridad.

Disponibilidad

La disponibilidad informática es la característica o capacidad de asegurar la fiabilidad y el acceso oportuno a los datos y recursos que los soportan por parte de los individuos autorizados, es decir, que lo necesitan para desenvolver sus actividades.

DLP

DLP o su significado en español significa, prevención de pérdida de datos, sirve para garantizar que los usuarios no envíen información delicada o crítica fuera de la red corporativa. El término describe productos de software que ayudan a un administrador de redes a controlar los datos que los usuarios pueden transferir.

DNSSEC (Domain Name System Security Extensions)

Conjunto de extensiones al protocolo DNS que proporcionan mecanismos para verificar la autenticidad y la integridad de los datos DNS, protegiendo contra ciertos tipos de ataques, como la suplantación de identidad de sitios web.

EDR (Respuesta y detección de endpoint)

Soluciones de seguridad que monitorizan y responden a amenazas en los dispositivos finales. Proporciona visibilidad y protección avanzada contra ataques dirigidos a 'endpoints' como computadoras portátiles, teléfonos móviles y servidores.

Envenenamiento del DNS (DNS spoofing)

Ataque en el cual se introducen datos corruptos en la caché de un servidor DNS, haciendo que las consultas DNS devuelvan direcciones IP incorrectas, redirigiendo así el tráfico a sitios maliciosos.

Equipo rojo

Equipo rojo se compone por profesionales de la seguridad informática que actúan como amenazas que intentan superar los controles.

escaneo de vulnerabilidades

Los **escaneo de vulnerabilidad** son herramientas de **software** o **hardware** que se utilizan para diagnosticar y analizar los ordenadores conectados a la red, lo que te permite examinar las redes, los ordenadores y las aplicaciones en busca de posibles problemas de seguridad, así como evaluar y corregir las vulnerabilidades.

A través de estas se pueden comprobar varias aplicaciones de un sistema en busca de posibles puntos débiles que puedan ser explotados por los atacantes, como las herramientas de bajo nivel y los escáneres de puertos

Esteganografía

La esteganografía es la práctica de ocultar información dentro de otro mensaje u objeto físico para evitar su detección. Se puede usar para ocultar casi cualquier tipo de contenido digital, ya sea texto, imágenes, videos o audios. Luego, dichos datos ocultos se extraen en destino.

F

Filtrado de paquetes

El filtrado de paquetes implica examinar cada paquete de red que pasa a través del firewall y tomar decisiones sobre si permitir o negar su paso según reglas de seguridad predefinidas.

Firma antivirus

En materia de riesgos cibernéticos, es un archivo que proporciona información al software antivirus para encontrar y reparar los riesgos. Sirve de protección contra el malware conocido.

Firma electrónica

La **firma electrónica** es un concepto jurídico, equivalente electrónico al de la firma manuscrita, donde una persona acepta y da por validado el contenido de un mensaje electrónico a través de cualquier medio electrónico que sea legítimo y permitido.

Footprint

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.

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

G

Gestión de incidentes

La gestión de incidentes es un proceso estructurado que maneja la respuesta a incidentes de seguridad informática. Su objetivo es limitar el daño causado por incidentes, recuperar rápidamente la normalidad operativa y reducir el riesgo de futuros incidentes a través del aprendizaje y la mejora continua.

Pasos: Identificación del incidente, contención, erradicación, recuperación y análisis post-incidente para extraer lecciones aprendidas y aplicar mejoras.

Gestor de contraseñas

Herramienta que ayuda a los usuarios a almacenar y gestionar sus contraseñas de manera segura, generando contraseñas fuertes y únicas para cada cuenta y manteniéndolas en una base de datos cifrada.

H

Hacker

Aquella persona que trata de solventar, paliar o informar sobre los problemas de seguridad encontrados en programas, servicios, plataformas o herramientas.

Hacktivista

Individuo o grupo que utiliza técnicas de hacking con el objetivo de promover causas políticas, sociales o ideológicas. El hacktivismo combina la programación y la piratería informática con el activismo político.

Heartbleed

Es un agujero de seguridad de *software* en la biblioteca de código abierto OpenSSL, solo vulnerable en su versión 1.0.1f, que permite a un atacante leer la memoria de un servidor o un cliente

Honeypot

Un *honeypot*, o sistema **trampa** o **señuelo**, es una herramienta de la seguridad informática dispuesto en una red o sistema informático para ser el objetivo de un posible ataque informático, y así poder detectarlo y obtener información del mismo y del atacante.

La característica principal de este tipo de programas es que están diseñados no solo para protegerse de un posible ataque, sino para servir de señuelo invisible al atacante, con objeto de detectar el ataque antes de que afecte a otros sistemas críticos. El *honeypot*, sin embargo, puede estar diseñado con múltiples objetivos, desde simplemente alertar de la existencia del ataque u obtener información sin interferir en el mismo, hasta tratar de ralentizar el ataque —*sticky honeypots*— y proteger así el resto del sistema

Honeytoken

Información o archivo falsos creados para atraer a atacantes, permitiendo a los administradores identificar y estudiar comportamientos maliciosos. Los honeytokens pueden parecer datos valiosos, pero su propósito es alertar a los administradores de posibles intentos de acceso no autorizado.

Los 'honeytoken' son señuelos que se colocan en lugares estratégicos (repositorios de archivos, bases de datos, servicios de correo, servicios web, etc.) pero que realmente no contienen ningún valor legítimo o información útil, y sobre los que se pone un sistema de vigilancia sobre su acceso, para descubrir posibles atacantes, monitorizar y auditar su actividad mediante técnicas forenses informáticas.



HTTP

El protocolo de transferencia de hipertexto (HTTP) es un protocolo o conjunto de reglas de comunicación para la comunicación cliente-servidor. Cuando visita un sitio web, su navegador envía una solicitud HTTP al servidor web, que responde con una respuesta HTTP. Es la tecnología subyacente que impulsa la comunicación de red.

HTTPS

El **protocolo de transferencia de hipertexto seguro** (HTTPS) es la versión segura de HTTP, que es el principal protocolo utilizado para enviar datos entre un navegador web y un sitio web. El HTTPS está encriptado para aumentar la seguridad de las transferencias de datos.

I

IDS

Es un software de seguridad cuya función es detectar accesos no autorizados en un sistema o una red de ordenadores, y en base a ello, generar algún tipo de alerta o log para que posteriormente pueda ser gestionado por el administrador de sistemas correspondiente.

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.

Indicadores de compromiso

Es un conjunto de datos sobre un objeto o una actividad que indica acceso no autorizado al equipo (compromiso de datos). Por ejemplo, muchos intentos fallidos de iniciar sesión en el sistema pueden constituir un indicador de compromiso. La tarea *Análisis de IOC* permite encontrar indicadores de compromiso en el equipo y tomar medidas de respuesta ante amenazas.

Información sensible

Cualquier dato que, si se difunde, podría resultar perjudicial para personas u organizaciones. Este tipo de información requiere estrictas medidas de protección debido a su carácter privado o confidencial. Por su importancia para la privacidad deben ser tratados y almacenados con un mayor cuidado y cumpliendo una serie de requisitos.

Informática forense

La informática forense, también conocida como ciencia forense digital, ciencia de la informática forense o ciberforense, combina la informática y la ciencia forense legal para recopilar pruebas digitales de una manera que sea admisible en un tribunal de justicia.

Infraestructura crítica

Las infraestructuras críticas son los sistemas físicos y las redes de información que ofrecen servicios esenciales para el funcionamiento y la seguridad de una organización, una ciudad o un país. Esto incluye transporte, comunicaciones, agua, sistemas de energía, internet, finanzas y gobierno, entre otros.

Infraestructura de clave pública

Una infraestructura de Clave Pública es un conjunto de protocolos, servicios y estándares que soportan aplicaciones basadas en criptografía de clave pública.

Algunos de los servicios ofrecidos por una ICP son los siguientes:

- Registro de claves.
- Revocación de certificados.
- Selección de claves.
- Evaluación de la confianza.
- Recuperación de claves.

Ingeniería Inversa

La ingeniería inversa es el proceso llevado a cabo con el objetivo de obtener información o un diseño a partir de un producto u objeto, con el fin de determinar cuáles son sus componentes y de qué manera interactúan entre sí y cuál fue el proceso de fabricación.

Ingeniería social

Método de ataque que utiliza la manipulación psicológica de las personas para que divulguen información confidencial o realicen acciones que comprometan la seguridad.

Insider

Un insider es un individuo que filtra, modifica o borra información privilegiada acerca de la empresa o marca en la que trabaja.

Inundación ICMP

La inundación de ICMP (Protocolo de Mensajes de Control de Internet) es un ataque cibernético que inunda un sistema objetivo con un gran volumen de paquetes de solicitud de eco ICMP (ping). Estos paquetes abrumarán los recursos del sistema, causando que se vuelva lento o no responda al tráfico de red legítimo.

Inyección de código

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.

IoT

Internet de las cosas, se refiere a la red colectiva de dispositivos conectados y a la tecnología que facilita la comunicación entre dispositivos y la nube, así como entre los propios dispositivos.

J

Jailbreak

Proceso mediante el cual se superan las restricciones del dispositivo, lo que permite al usuario cambiar el sistema operativo o la instalación de ciertas aplicaciones.

K

Kerberos

Un Kerberos es un sistema o enrutador que proporciona una puerta de enlace entre los usuarios e Internet. Por lo tanto, ayuda a evitar que los ciberatacantes ingresen a una red privada

Keylogger

Un keylogger es un hardware o software malicioso que, sin tu permiso o conocimiento, registra todas las teclas que pulsás para operar tu computadora o celular.

L

LAN

Area local de ordenadores conectados entre si en un area determinada, permite el cambio de datos y comunicación entre los dispositivos conectados.

Lista blanca

Mas conocido como White list, es un metodo de bloqueo por el que sólo permite a determinadas direcciones de correos electrónicos o nombres de dominio autorizados pasar por el software de seguridad

Log

Término registro, log o historial de log para referirse a la grabación secuencial en un archivo o en una base de datos de todos los acontecimientos (eventos o acciones) que afectan a un proceso particular (aplicación, actividad de una red informática, etc.).

Login

Se define como iniciar sesión o conectarse ('llevar a cabo las acciones necesarias para empezar a utilizar un sistema informático'), y que a veces incluso equivale a registrarse.

LOPDGDD

La Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales tiene como objetivo proteger los datos personales y garantizar los derechos digitales de los usuarios. Según esta ley, las empresas tienen la responsabilidad de establecer medidas de seguridad adecuadas para garantizar la protección de los datos personales y cumplir con una serie de obligaciones.

LSSI-CE

Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico. La LSSI tiene como fin proteger a los consumidores de servicios electrónicos, entre los que se incluye el comercio electrónico o las tiendas online.

M

Malware

El malware, abreviatura de "software malicioso", es **cualquier código de software o programa informático escrito de manera intencionada para dañar un sistema informático o a sus usuarios.**

MAM (Mobile Application Management)

Proceso y tecnologías utilizadas para gestionar y asegurar aplicaciones móviles utilizadas dentro de una organización. MAM permite a los administradores controlar el acceso a las aplicaciones, distribuir actualizaciones y garantizar la seguridad de los datos corporativos.

Medio de propagacion

se refiere a la forma en que se propaga o se distribuye un virus informático, malware u otro tipo de software malicioso. Es importante entender cómo se propaga una amenaza ya que, sin esta comprensión, la eliminación y prevención de su propagación puede resultar difícil.

Mitigación

La mitigación es el proceso de identificar vulnerabilidades potenciales en los sistemas y redes informáticos y, a continuación, aplicar medidas de seguridad para reducir o eliminar su efecto. Estos procesos suelen implicar la aplicación de parches, el endurecimiento y el uso de configuraciones seguras.

N

No repudio

No repudio se refiere a un **estado de negocios donde el supuesto autor de una declaración no es capaz de desafiar con éxito la validez de declaración o contrato**. El término es a menudo visto en un entorno legal donde la autenticidad de una firma está siendo desafiada.

P

P2P

Una red P2P o 'peer to peer' es un tipo de conexión con una arquitectura destinada a la comunicación entre aplicaciones. Esto permite a las personas o a los ordenadores compartir información y archivos de uno a otro sin necesidad de intermediarios.

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

Las pasarelas de pago son portales online donde se conecta una cuenta bancaria con un procesador de pagos informático que permite verificar, aceptar o rechazar las transacciones realizadas a través de un ecommerce

Pentest (Penetration Testing)

Prueba de penetración o evaluación de seguridad en la que expertos simulan ataques cibernéticos para identificar vulnerabilidades en sistemas, redes o aplicaciones. El objetivo es descubrir y corregir debilidades antes de que puedan ser explotadas por atacantes reales.

PGP

PGP (Pretty Good Privacy) se ha convertido en un pilar de la privacidad y la seguridad por una razón principal de Internet: que te permite enviar un mensaje cifrado a alguien sin tener que compartir el código de antemano. Hay mucho más, pero este es el aspecto fundamental que lo ha hecho tan útil.

Supongamos que necesitas enviar un mensaje confidencial a un amigo sin que nadie más descubra su contenido. Una de las mejores soluciones sería alterarlo con un código secreto que solo tú y tu amigo conozcan, de modo que si alguien intercepta el mensaje, no pueda leer el contenido.

Pharming

Ciberataque que intenta redirigir datos especialmente los de solicitud a un sitio web fraudulento sin autorización.

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

Ping

Es una herramienta de diagnóstico de red que se utiliza para determinar la comunicación.

Plan de continuidad (BCP)

Plan que define los pasos que se requieren para el Restablecimiento de los Procesos de Negocio después de una interrupción. El Plan también identifica los disparadores para la Invocación, las personas involucradas, las comunicaciones, etc. El Plan de la Continuidad del Servicio TI es una parte importante de los Planes de Continuidad del Negocio

Plan Director de Seguridad

Un Plan Director de Seguridad consiste en la definición y priorización de un conjunto de proyectos 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 (PDS),

que se alinee con los objetivos estratégicos de la empresa, incluya una definición del alcance e incorpore las obligaciones y buenas prácticas de seguridad que deberán cumplir los trabajadores de la organización así como terceros que

colaboren con ésta.

Plugin

Son pequeños programas complementarios que amplían las funciones de aplicaciones web y programas de escritorio. Por norma general, cuando instalamos un plugin, el software en cuestión adquiere una nueva función. La mayoría de los usuarios conoce los plugins por los navegadores web, aunque ya se han asentado en cualquier tipo de programa y aplicación.

Privacidad

Derecho y capacidad de una persona o entidad para controlar el acceso a su información personal y confidencial, así como la protección de esta información contra accesos no autorizados, usos indebidos o divulgaciones sin consentimiento.

Protocolo

Cuando hablamos de protocolo nos referimos a ese **conjunto de disposiciones y normas que permiten que los seres humanos sepan cómo relacionarse a nivel social y/o profesional en actos formales y oficiales.**

Proveedor de acceso (ISP)

Compañía que ofrece servicios de acceso a Internet a individuos y organizaciones, permitiéndoles conectarse a la red global.

Puerta trasera (Backdoor)

Backdoor es una puerta trasera para tomar el control de un equipo, casi siempre con intenciones ilegítimas, de manera remota y sin que el titular del mismo esté al tanto.

R

Ramsonware

Es un tipo de malware o código malicioso que impide la utilización de los equipos o sistemas que infecta. El atacante toma el control del equipo o sistema infectado y lo controla de varias maneras, cifrando la información, bloqueando la pantalla, etc...

Repudio

El no repudio es un principio de seguridad informática que se refiere a la situación en la que un remitente de información no puede negar haber enviado un mensaje o haber llevado a cabo una acción en particular.

Resiliencia

Es la capacidad de una organización de adaptarse a las amenazas cibernéticas sin interrumpir la integridad, la finalidad ni la continuidad del negocio. Representa el nivel de preparación de una empresa para adelantarse a los ataques cibernéticos, así como para detectarlos y recuperarse de ellos.

Respuesta de incidentes

Se refiere a la reacción ante un incidente cibernético. Esta respuesta puede llevarla a cabo el propio equipo de respuesta ante incidentes de la empresa (el administrador o departamento informático) o un proveedor de servicios externo. Es importante que la respuesta se efectúe lo más rápido posible.

RIFD

Identificación por Radio Frecuencia, es una tecnología que permite identificar objetos mediante ondas de radio de manera única y pudiendo captar cientos de objetos a la vez.

Rogue Access Point

Un rogue access point es cualquier punto de acceso inalámbrico que se encuentre dentro del alcance de la red y que no se reconoce como un punto de acceso autorizado, ni como una excepción configurada en la implementación inalámbrica.

Rooskit

Es un tipo de software malicioso diseñado para darle a un hacker la capacidad de introducirse en un dispositivo y hacerse con el control del mismo.

Rootear Android

Proceso de obtener permisos de superusuario (root) en dispositivos con el sistema operativo Android, lo cual permite modificar el software del dispositivo más allá de las restricciones impuestas por el fabricante.

Router

Un router es un dispositivo de red especializado encargado de reenviar paquetes de datos entre distintas redes informáticas.

S

SaaS

El software como servicio (SaaS) se considera tradicionalmente un modelo de software basado en la nube, el cual ofrece aplicaciones a los usuarios finales a través de un navegador de Internet. Los proveedores de SaaS alojan servicios y aplicaciones para que los clientes puedan acceder a ellos bajo demanda.

Sandbox

Protege en tiempo real los servidores de datos, y hace de control preventivo de la ejecución de código fuente, datos o contenido, evitando unos cambios que podrían ser perjudiciales (independientemente de la intención del autor de los mismos) para un sistema, o que simplemente, podrían ser cambios de difícil reversión.

Segmentación de red

Práctica de dividir una red informática en subredes más pequeñas y aisladas para mejorar el rendimiento, la seguridad y la administración. La segmentación permite limitar el acceso a ciertos recursos y contener posibles brechas de seguridad dentro de áreas específicas.

Seguridad por oscuridad

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.

Sello de confianza

Los sellos de confianza son la prueba visual del cifrado y la protección de identidad de un sitio web mediante un certificado TLS/SSL. Son el distintivo de confianza que proporcionan las autoridades de certificación u otras organizaciones para certificar que se trata de un sitio web legítimo.

Servidor

Un servidor es un sistema que proporciona recursos, datos, servicios o programas a otros ordenadores, conocidos como clientes, a través de una red. En teoría, se consideran servidores aquellos ordenadores que comparten recursos con máquinas receptoras.

Session Hijacking

Ocurre cuando un atacante logra control sobre la sesión activa de un usuario mediante el robo del identificador de la misma, resultando en la transgresión de los mecanismos de autenticación del servicio, y permitiendo al atacante realizar cualquier acción autorizada para esa determinada sesión.

SFTP

Abreviatura de Secure File Transfer Protocol (Protocolo de transferencia segura de archivos). Este protocolo permite transferir datos cifrados entre tu ordenador local y el espacio web del que dispones en tu hosting de STRATO a través de Secure Shell (SSH).

SGSI

SGSI es un Sistema de Gestión de Seguridad de la Información (Information Security Management System, por sus siglas en inglés). Un SGSI es un conjunto de principios o procedimientos que se utilizan para identificar riesgos y definir los pasos de mitigación de riesgos que deben llevarse a cabo.

Shadow IT

Se refiere a cualquier tipo de software o hardware utilizado dentro de una empresa que no cuenta con la aprobación ni el control del área de Tecnología de la Información de la organización.

SIEM

La Administración de eventos e información de seguridad, SIEM, para abreviar, es una solución de seguridad que ayuda a las organizaciones a detectar y analizar amenazas y responder a ellas antes de que afecten a las operaciones del negocio.

Sistemas de reputación

Herramientas y mecanismos que evalúan y asignan una calificación de reputación a usuarios, direcciones IP, dominios u otros elementos basados en su comportamiento y actividades previas. Se utilizan para detectar y prevenir actividades maliciosas, como el spam y el fraude.

SMTP

El protocolo simple de transferencia de correo (SMTP) es un protocolo TCP/IP que se utiliza para enviar y recibir correo electrónico. Normalmente se utiliza con POP3 o con el protocolo de acceso a mensajes de Internet (IMAP) para guardar mensajes en un buzón del servidor y descargarlos periódicamente del servidor para el usuario.

Sniffer

También denominado rastreador de red, es un software o hardware que se utiliza para monitorizar, capturar y analizar en tiempo real los paquetes de datos que pasan por una red, sin redirigirlos ni alterarlos. Aunque originalmente no es una herramienta maliciosa, es posible utilizarla como tal.

Spear phishing

Se trata de ciber ataques altamente personalizados, dirigidos a personas o empresas concretas, mediante correos electrónicos, aparentemente seguros para el destinatario que lo incitan a compartir datos confidenciales con el atacante

Spoofing

Técnica utilizada para falsificar la identidad de una fuente, ya sea una dirección IP, una dirección de correo electrónico, o un sitio web, con el fin de engañar a los usuarios y obtener acceso no autorizado a información o sistemas.

Spyware

Malware que recopila información de un ordenador afectado y después lo transmite a una entidad externa no autorizada.

SSID (Service Set Identifier)

Nombre único que identifica a una red inalámbrica. Los dispositivos usan el SSID para conectarse a la red específica en un área donde hay múltiples redes inalámbricas disponibles.

T

TCP/IP

TCP/IP son las siglas de Transmission Control Protocol/Internet Protocol (que significa Protocolo de Control de Transmisión/Protocolo de Internet).

Texto plano

El texto plano es cualquier texto o información que no ha sido cifrado o encriptado de ninguna manera. Es decir, se trata de texto que puede ser leído y comprendido directamente, sin necesidad de desencriptarlo.

Troyano

Tipo de software malicioso que se disfraza como un programa legítimo o inofensivo para engañar a los usuarios y obtener acceso no autorizado a sus sistemas. Una vez instalado, puede ejecutar acciones dañinas, como robar datos o instalar otros tipos de malware.

Túnel

Se conoce como túnel o tunneling a la **técnica que consiste en encapsular un protocolo de red sobre otro** (protocolo de red encapsulador) creando un túnel de información dentro de una red de computadoras.

U

UTM

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.

V

Virus

Un **virus informático** es un software que tiene por objetivo alterar el funcionamiento normal de cualquier tipo de dispositivo informático, sin el permiso o el conocimiento del usuario principalmente para lograr fines maliciosos sobre el dispositivo. Los virus, habitualmente, reemplazan archivos ejecutables por otros infectados con el código de este mismo. Los virus pueden destruir, de manera intencionada, los datos almacenados en una computadora, aunque también existen otros más inofensivos, que solo producen molestias o imprevistos.

VLAN

Virtual Local Area Network o Red de Área Local Virtual- es una división de red que se realiza de forma virtual. Como su nombre indica, la técnica consiste en crear una red virtual dentro de un único dispositivo, normalmente un switch.

Una VLAN permite que una red de computadoras y usuarios se comuniquen en un entorno simulado como si existieran en una sola LAN y estuvieran compartiendo un solo dominio de transmisión y multidifusión.

VoIP

El término VoIP significa "Voice Over Internet Protocol" en inglés, que al castellano se traduce como Voz Sobre Protocolo de Internet y se trata de una tecnología que permite realizar y recibir llamadas de voz a través de la red.

W

WPA

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 estinado 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).

WPS

Las siglas WPS significan Wifi Protected Setup, y es un sistema que tiene por funcionalidad básica la de ofrecer una manera controlada de conectarse a una Wi-Fi escribiendo sólo un PIN de 8 dígitos en lugar de la contraseña inalámbrica completa.

X

XSS (Secuencias de comandos en sitios cruzados)

Una secuencia de comandos en sitios cruzados o Cross-site scripting (XSS) es un tipo de ataque informático que permite a un actor de amenazas ejecutar código malicioso en el navegador de otro usuario. Ocurren cuando una aplicación web utiliza la entrada de un usuario sin validarla adecuadamente. Esto puede resultar en el robo de cookies, tokens de sesión y otra información confidencial.

Z

Zero-day (0-day)

Un **ataque de día cero** (en inglés: *zero-day attack*) es un ataque contra una aplicación o sistema informático que tiene como objetivo la ejecución de código malicioso gracias al conocimiento de vulnerabilidades que son desconocidas para los usuarios y para el fabricante del producto. Esto supone que aun no hayan sido arregladas. Es frecuente la venta en el mercado negro de exploits que aprovechan estas vulnerabilidades. Su precio se establece con base a su impacto y el número de dispositivos vulnerables. Un ataque de día cero se considera uno de los más peligrosos instrumentos de una guerra informática.



Compromiso de calidad

El grupo Centro de Formación Master tiene un sincero compromiso con la gestión de calidad con el fin de mejorar continuamente los productos formativos y servicios que ofrecemos. Todas las medidas y acciones que realizamos están destinadas a poder ofrecer los mejores cursos cumpliendo con nuestro lema "La Formación por Excelencia".

[Leer más](#)

[Resumen de retención de datos](#) [Descargar la app para dispositivos móviles](#)

© 2023 - 2024 Centro de Estudios Master. All rights reserved.

