GLOSARIO

DE TÉRMINOS DE CIBERSEGURIDAD

REPÚBLICA :DIGITAL

CNCS | CENTRO NACIONAL DE CIBERSEGURIDAD
REPÚBLICA DOMINICANA

ÍNDICE

GLOSARIO DE TÉRMINOS DE CIBERSEGURIDAD

CNCS CENTRO NACIONAL DE CIBERSEGURIDAD REPÚBLICA DOMINICANA

DEFINICIONES

Amenaza: Circunstancia desfavorable que puede ocurrir y que cuando sucede tiene consecuencias negativas sobre los activos provocando su indisponibilidad, funcionamiento

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

Activo de Información: Cualquier información o sistema relacionado que tenga valor para la organización

Adware: Software que muestra automáticamente anuncios al usuario durante la instalación o durante el uso de algún sistema que genera ganancia para los creadores.

Amenaza: Situación nociva que puede suceder y cuando sucede tiene consecuencias negativas sobre los activos de información afectando su funcionamiento.

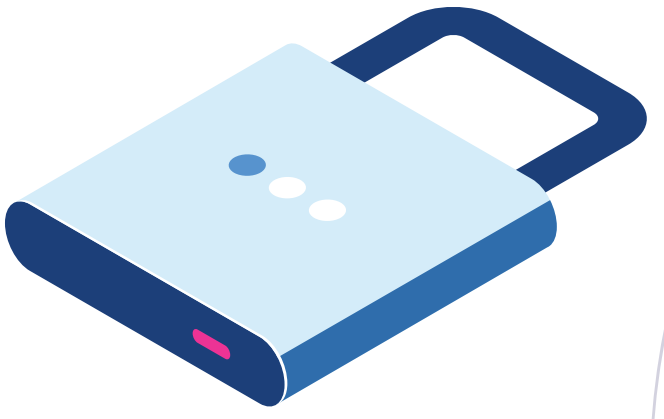
Antivirus: Es un programa informático que sirve para evitar o combatir las infecciones provocadas por un código malicioso.

Análisis de Riesgo: Es el proceso que busca identificar los activos de información, sus vulnerabilidades y amenazas, así como la probabilidad de ocurrencia y el impacto de las mismas, con el objetivo de determinar los controles adecuados.

Autenticación: Procedimiento que permite identificar que alguien es quien dice ser cuando accede a los sistemas de información.

Autoridad de Certificación (CA): Autoridad de confianza cuyo objetivo es garantizar la identificacion de los titulares de certificados digitales y la correcta asociación a la firma digital.

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.



B2B: Abreviatura de “Business to Business”. Este término se refiere a las transacciones comerciales entre empresas, utilizando medios telemáticos.

B2C: Abreviatura de “Business to Consumer”. Este término se refiere a la estrategia que desarrollan las empresas comerciales para llegar directamente al cliente o consumidor final.

Backdoor o Puerta trasera: Error o fallo del Sistema de información que permite a una persona acceder al Sistema sin autorización, de igual forma puede ser creada por el ciberatacante para utilizarlo de forma ilícita.

BIA: Business Impact Analysis informe donde se muestre el costo de interrupción de los procesos críticos del negocio.

Bomba Lógica: inserción de código intencionalmente en un Sistema para que se ejecute al momento de cumplir una o más condiciones preprogramadas.

Botnet: Conjunto de ordenadores controlados de forma remota por un ciberatacante que puede utilizar para acciones maliciosas.

Ciberespacio: Es un ambiente compuesto por las infraestructuras tecnológicas, los componentes lógicos de la información y las interacciones sociales que se verifican en su interior.

Ciberseguridad: Es tanto una condición caracterizada por un mínimo de riesgos y amenazas a las infraestructuras tecnológicas, los componentes lógicos de la información y las interacciones que se verifican en el ciberespacio, como el conjunto de políticas y técnicas destinadas a lograr dicha condición.

Cibercrimen: Son los actos delictuales donde el ciberespacio es el objeto del delito o su principal herramienta para cometer ilícitos contra individuos, organizaciones, empresas o gobiernos.

Certificado Digital: Archivo generado por la Autoridad Certificadora que relaciona los datos de la persona física con su identidad digital, es válido para autenticar y validar del usuario o sitio web.

Cifrado: Método que permite aumentar la seguridad de un mensaje mediante la codificación del contenido de manera que solo pueda tener acceso la persona autorizada.

Cloud Computing o Computadora en la Nube: Modelo que permite ofrecer servicios a través de internet. Es una nueva tecnología que busca tener todos los activos de información en la internet sin preocuparse por espacio y capacidad de procesamiento en nuestros dispositivos locales.

Confidencialidad: Es la propiedad de la información que permite garantizar que es accesible solo pero el personal autorizado

Control parental: Herramientas que permiten establecer controles para la navegación de los menores de edad, controlando las herramientas a instalar y páginas web a visitar.

Cookies: Pequeños archivos que almacenan las informaciones de la navegación enviadas por el sitio web y son almacenadas en el equipo de usuario.

Contrafuego: (Firewall) Sistema de seguridad que tiene como objetivo permitir o denegar el acceso a la red desde diferentes ámbitos para proteger la infraestructura.

Criptografía: Es un método de ocultación de mensaje que para que el mismo resulte ilegible a todo aquel que no conozca el sistema por el cual ha sido cifrado.

Denegación de Servicio: En términos de seguridad informática es un conjunto de técnicas que tienen como objetivo dejar inoperativo un servidor, realizando una sobrecarga de peticiones ilegitimas.

Dirección IP: Número único e irrepetible para identificar los sistemas conectados. Existen dos tipos “Publicas” que pueden ser accesibles desde cualquier Sistema conectado a internet o “Privadas” que pueden ser accesibles desde las redes internas.

Dirección MAC: Valor único e irrepetible que contiene 48 bits e identifica todos los dispositivos conectados en la red.

Disponibilidad: Capacidad de un Sistema de ser accesible y utilizable cuando sea requerida por los usuarios y es uno de los pilares de la seguridad de la información.

Exploit: Es una estructura de comandos que se utilizan para aprovechar una vulnerabilidad en un sistema de información con el objetivo de alterar su funcionamiento.

Gusano: Programa malicioso con propiedad de duplicarse a sí mismo sin la intervención del usuario y aprovechando todo tipo de medio disponible.

Incidente Cibernético: evento que afecta la confidencialidad, integridad o disponibilidad de la información, como también la continuidad del servicio proporcionado por los sistemas que la contienen.

Infraestructura crítica de la información: Las instalaciones, redes, servicios y equipos físicos y de tecnología de la información cuya afectación, degradación, denegación, interrupción o destrucción pueden tener una repercusión importante en la salud, la seguridad o el bienestar económico de los ciudadanos o en el eficaz funcionamiento de los gobiernos de los Estados.

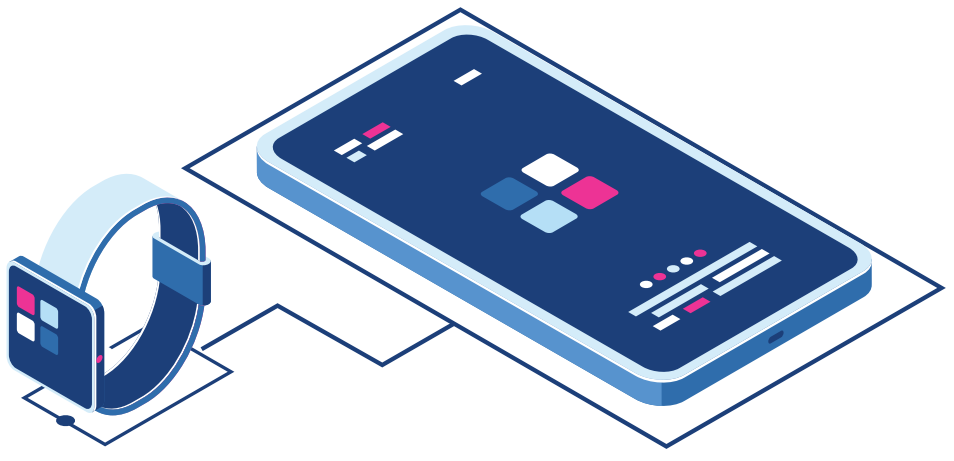
IDS: Intrusion Detection System en inglés, es u Sistema utilizado para detectar los accesos no autorizados a los equipos o a la red. Los accesos pueden ser producto de un ciberatacante.

Incidente de Seguridad: Suceso que afecta los pilares de la ciberseguridad que son confidencialidad, integridad y disponibilidad de los activos de información.

Ingeniería social: Técnicas usadas por los ciberatacantes para obtener informaciones confidenciales o sensible de una persona, esta técnica suele ser efectiva ya que utiliza la buena voluntad de los usuarios y los varios métodos de persuasión.

Integridad: Propiedad de la información que garantiza la exactitud de los datos enviados para asegurar que no se han realizado alteraciones, perdida o destrucción al momento de la transferencia o almacenamiento.

Inyección SQL: Es un ataque que aprovecha una vulnerabilidad en el proceso de validación de la introducción de contenido en un formulario web que permite el robo de las credenciales de la base de datos.



Malware: Programa malicioso que tiene como objetivo dañar, robar o introducirse al sistema sin ser detectado por el usuario. Existen varios tipos de programas maliciosos; virus, troyanos, spyware, entre otros.

Parche de Seguridad: Conjunto de cambios que son aplicados a un programa para subsanar un error de seguridad..

Política de Seguridad: son las medidas de seguridad que han sido establecidos en una organización para mantener la seguridad de sus sistemas de información, luego de evaluar sus activos de información y los riesgos a los que se encuentran expuestos.

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

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

SaaS: Software as a Service, es un modelo de distribución de software donde tanto los programas como los datos son almacenados en una estructura de terceros.

Sniffer: Es un programa que permite monitorizar la red desactivando el proceso de validación que hace la tarjeta de red para determinar si el paquete va dirigido o no al equipo.
Spyware; programa malicioso que recopila información de un equipo para ser enviada sin autorización del propietario a otro destino.

Suplantación de Identidad: Actividad realizada por un ciberatacante para realizar actividades ilícitas haciéndose pasar por otra persona.

Sistema informático: Todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de alguno de sus elementos, sea el tratamiento automatizado de datos en ejecución de un programa 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.

SMTP: El Protocolo Simple de Transferencia de Correo (o Simple Mail Transfer Protocol del inglés) es un protocolo de red utilizado para el intercambio de mensajes de correo electrónico. Este protocolo, aunque es el más comúnmente utilizado, posee algunas limitaciones en cuanto a la recepción de mensajes en el servidor de destino (cola de mensajes recibidos).

Sniffer: Programa que monitoriza la información que circula por la red con el objeto de capturar información.

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

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

- **IP spoofing**: Consiste en la suplantación de la dirección IP de origen de un paquete TCP/IP por otra dirección IP a la cual se desea suplantar.

- **ARP spoofing**: Es la suplantación de identidad por falsificación de tabla ARP. ARP (Address Resolution Protocol) es un protocolo de nivel de red que relaciona una dirección MAC con la dirección IP del ordenador. Por lo tanto, al falsear la tabla ARP de la víctima, todo lo que se envíe a un usuario, será direccionado al atacante.

- **DNS spoofing**: Es una suplantación de identidad por nombre de dominio, la cual consiste en una relación falsa entre IP y nombre de dominio.

- **Web spoofing**: Con esta técnica el atacante crea una falsa página web, muy similar a la que suele utilizar el afectado con el objetivo de obtener información de dicha víctima como contraseñas, información personal, datos facilitados, páginas que visita con frecuencia, perfil del usuario, etc. Los ataques de phishing son un tipo de Web spoofing.

- **Mail spoofing**: Suplantación de correo electrónico bien sea de personas o de entidades con el objetivo de llevar a cabo envío masivo de spam.

Virtualización: Es la creación de un dispositivo en su versión virtual con el apoyo de programas que aplican capas de abstracción en la maquina física para compartir los recursos.

Vulnerabilidad; deficiencias de un programa que pueden permitirle a un ciberatacante acceder a información no permitidas.

Zero day: Vulnerabilidades en sistemas o programas que son únicamente conocidas por un grupo de atacantes y los fabricantes no tienen conocimiento de las mismas.

Zombie: Denominación para identificar a los computadores controlados de manera remoto por un ciberatacante mediante la infección por malware. El equipo es utilizado para realizar actividades ilícitas mediante la red.

REPÚBLICA
:DIGITAL

CNCS | CENTRO NACIONAL
DE CIBERSEGURIDAD
REPÚBLICA DOMINICANA