AMENAZAS, ATAQUES Y VULNERABILIDADES

Capacítate para el empleo | FUNDACIÓN Carlos Slim

La operación continua y adecuada del sistema informático **encara vulnerabilidades** provenientes de amenazas del entorno y ataques externos.

! VULNERABILIDADES

Son **debilidades en el sistema informático,** en la estrategia de seguridad, en los controles internos o en su implementación; que **son explotadas por una fuente de amenazas.**

Éstas se dividen en:

FÍSICA

Es el **ingreso sin consentimiento** y directa a los equipos del sistema, para obtener su información, alterarla o destruirla.

NATURAL

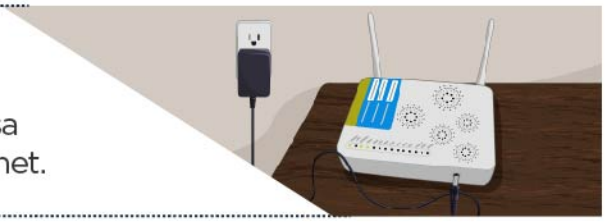
Son los **daños que sufre el sistema** debido a causas ambientales, como incendios e inundaciones.

SOFTWARE

Llamado también *bugs*, es el **acceso al sistema debido a fallas** en su diseño de programación.

DE COMUNICACIONES

Son **accesos no autorizados** al sistema de la empresa de usuarios conectados en una red pública como internet.



HUMANA

Son los **errores causados por los administradores y usuarios** de la empresa en sus sistemas, como son configuraciones y manejo de los estaciones de trabajo incorrectos.

AMENAZAS

Es un evento que **puede producir daños en los activos del sistema informático;** lo pueden provocar usuarios internos o ajenos a la empresa. Cualquier sistema informático **está expuesto a las siguientes amenazas:**

Actos criminales o motivados por la política organizacional, llamadas también **amenazas externas:** su origen es humano y en muchas ocasiones explotan las vulnerabilidades derivadas de la ausencia o deficiencia de controles de acceso y autenticación, así como la detección y prevención de intrusos. Algunas son:

- Robo físico
- Espionaje digital
- Allanamiento físico
- Sabotaje
- Infiltración
- Violación de derechos de autor
- Extorsión

Las personas externas que buscan corromper la seguridad **se clasifican en:**

AFICIONADOS

Tienen pocas habilidades en desarrollo de ataques por lo que usan herramientas que se encuentran en internet. Aunque sus acciones son básicas, el daño que provocan puede ser devastador.

HACKERS

Penetran en las computadoras o redes por varios motivos, lo que los divide en:

De sombrero blanco

Descubren debilidades con el fin de mejorar la seguridad.

De sombrero negro

Obtienen ganancias por encontrar una vulnerabilidad.

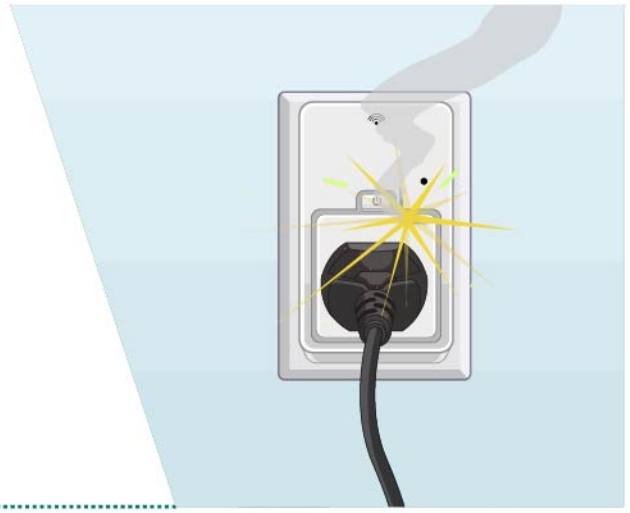
De sombrero gris

Son la combinación de los anteriores.

HACKERS ORGANIZADOS

Son organizaciones de delincuentes informáticos como "hacktivistas", terroristas y grupo patrocinados por organizaciones; cuyo objetivo es el control de sistemas en sectores como el energético.

Incidentes de origen físico. Están fuera del control humano, derivados la influencia inherente de factores ambientales y sólo mitigados con medidas preventivas:



- Incendios, sismos y desastres naturales
- Sobrecargas en la red eléctrica
- Fallas eléctricas
- Fallas circunstanciales en los sistemas

Negligencia y malas decisiones, llamadas también **amenazas internas.** Son difíciles de predecir debido a su origen humano no intencional y provienen de personas que tienen influencia sobre los sistemas en su constitución u operación. Éstas incluyen:

- Mal manejo de sistemas y herramientas
- Uso de *software* no autorizado
- Eliminación accidental de datos
- Infección de sistemas
- Transmisión no cifrada de datos críticos
- Exposición o extravío de equipo, unidades de almacenamiento, etcétera
- Falta de definición de perfil, privilegios y restricciones del personal

ATAQUES

Entre los principales **ataques a los sistemas de información** que utilizan los *hackers*, se encuentran:

Ataque distribuido de denegación de servicio o (DDoS)

Agobia los recursos de los sistemas por lo que **se ven imposibilitados para responder a las solicitudes de servicio** por parte de sus usuarios. Entre sus tipos están el de hundimiento, lágrima y *ping* de la muerte.

FUNDAMENTOS DE SEGURIDAD INFORMÁTICA Nivel 1

AMENAZAS, ATAQUES Y VULNERABILIDADES

Capacítate para el empleo | FUNDACIÓN Carlos Slim

Phishing

Es el **envío de correos electrónicos** que aparentan ser de una fuente confiable **con la finalidad de obtener información personal** o de influir en las acciones del usuario. Éste puede involucrar correos con archivos adjuntos que cargan *software* malicioso.

Inyección SQL

Es un **método de ingreso de código malicioso a la base datos** para leer y modificar información sensible, como la administrativa. Esto mediante la ejecución de una solicitud SQL a la base de datos, por medio de una entrada de información desde el cliente al servidor.

Código malicioso

Tiene el propósito de **atacar las plataformas digitales,** entre ellos están:

TROYANO

Es un **programa que se hace pasar por otro.** Una vez que el usuario lo instala por error, **permite que un tercero tome el control de su computadora.** Normalmente un troyano se utiliza para instalar otro *malware* de control como *keyloggers*, puertas traseras o para ejecutar *exploits.*

ROOTKIT

Es un programa que **otorga permisos al atacante para actuar como si fuera el usuario** administrador de la PC victima. Comúnmente, esconden su apariencia con programas inofensivos, como las herramientas de *software* de oficina. Usan un *exploit* o un troyano para poder ejecutarse.

ROGUE/SCAREWARE

Mejor conocidos como "falsos antivirus". Son aplicaciones que se instalan en el sistema y venden mediante anuncios falsos *software* que supuestamente desinfecta el equipo. Son difíciles de eliminar y suelen provocar problemas de rendimiento en el cómputo.

FUNDAMENTOS DE SEGURIDAD INFORMÁTICA Nivel 1

AMENAZAS, ATAQUES Y VULNERABILIDADES

Capacítate para el empleo | FUNDACIÓN Carlos Slim

EXPLOITS

Son **programas que "explotan" los fallos o debilidades de los programas,** como errores de codificación o *bugs*.

WORMS

Son *software* que reciben el nombre de gusanos informáticos, ya que **se expanden por los archivos de la computadora,** con lo que afectan el rendimiento e imposibilitan el trabajo.

SPYWARE

Es un programa que **recopila datos, sin consentimiento del usuario,** y generalmente se esconden dentro de publicidad y actualizaciones. Un *keylogger* puede ser un tipo particular de *spyware*.

KEYLOGGERS

Son programas que **registran la actividad del teclado y la envían al atacante,** quien roba contraseñas e información personal, con fines de extorsión.

RANSOMWARE

Transforma los datos de los equipos de cómputo para que no sean entendibles, bloqueándolos y con ello una solicitud de un pago llega a la víctima para poder volver a su estado inicial.

BOTS

Permite que un intruso tome el control de un equipo (regularmente dispositivos inalámbricos con una deficiente seguridad) al automatizar tareas que el dueño generalmente haría.

PHARMING

Dirigen a la víctima a un sitio *web* falso con el propósito de **mostrar publicidad o robar datos sobre sus cuentas** en el momento que el usuario ingresa en esa página falsa.

ADWARE

Es la **filtración de ventanas publicitarias.** Por lo que no causa daños a las funciones de administración del sistema, pero dificulta el trabajo por constantes interrupciones.

BACKDOOR

Son **códigos introducidos en los programas** para lograr un control remoto de los mismos. También se les conoce como "puertas traseras".

Distinguir cada una de las posibles afectaciones de la infraestructura de cómputo de la empresa **te ayudará en la definición de los mecanismos de seguridad preventivos y correctivos.**