Conceptos sobre Seguridad

¿Qué es Seguridad?

La seguridad es un estado de confianza personal, por conocimiento o desconocimiento y se rompe ante la materialización de algún evento.

¡Nuestro objetivo es sentirnos seguros por conocimiento y NUNCA por desconocimiento!

Que es Información?

La información es un activo que como otros activos importantes tiene valor y requiere en consecuencia una protección adecuada.

La información puede estar:

- Impresa o escrita en papel.
- Almacenada electrónicamente.
- Trasmitida por correo o medios electrónicos
- Mostrada en filmes.
- Hablada en conversación.

.

La *Seguridad de la Información* tiene como fin la protección de los activos de información.

La seguridad absoluta es imposible, no existe un sistema totalmente seguro, de forma que el elemento de riesgo siempre está presente, pese a cualquier medida que tomemos, razón por la cual se debe hablar de niveles de seguridad.

¿Cuál es la diferencia entre la Seguridad Informática y la Seguridad de la Información?

Seguridad Informática:
Tiene como objetivo primario proteger las infraestructuras tecnológicas y de comunicación que soportan la operación de una organización (básicamente hardware y software).

Seguridad de la Información:
Tiene como objetivo principal proteger la información de una organización.

Principios de la Seguridad Informática

La **seguridad** de la información se define como el conjunto de medidas que previenen, corrigen, detectan para proteger la confidencialidad, la integridad y la disponibilidad de la información de un sistema.

Principios de la Seguridad Informática

La **confidencialidad** es la propiedad que impide la divulgación de información a personas o sistemas no autorizados

Riesgos:

-Acceso no autorizado a un documento
-Privilegios no controlados
-Datos en texto claro

Contramedidas:
- Admón. de usuarios y perfiles
- Cifrado de datos

Principios de la Seguridad Informática

La **Integridad** es la propiedad que busca mantener los datos libres de modificaciones no autorizadas. Es mantener con exactitud la información tal cual fue generada, sin ser manipulada o alterada por personas o procesos no autorizados

Riesgos

-Modificación o perdida de datos
-Falta de calidad de los datos

Contramedidas:
-Cifrado de datos
-Aseguramiento de la comunicación
-Antivirus

Principios de la Seguridad Informática

La **disponibilidad** es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones

Riesgos

-Caídas del sistema
-Eliminación de información

Contramedidas:
-Backup
-Plan de contingencia

Taller

Coloque el ejemplo de acuerdo a cada Característica de seguridad.

Confidencialidad	Integridad	Disponibilidad

- La base de datos de producción esta arrojando datos erróneos
- El Sub-gerente envía todos los archivos encriptados a la gerencia.
- Los usuarios del área financiera no pueden ingresar al sistema contable
- El técnico revisa todos los archivos de la USB con el antivirus
- La secretaria envió el balance contable a todos los empleados por error
- La empresa cuenta con un centro de datos alterno en caso de desastre
- Todos los empleados pueden ver el informe en la Intranet menos el Gerente general.

CONCEPTOS SOBRE SEGURIDAD

Amenaza: Una Amenaza es la posibilidad de ocurrencia de cualquier tipo de evento o acción que puede producir un daño (material o inmaterial) sobre los elementos de un sistema

Vulnerabilidad: Es una debilidad en el diseño o un error de implementación que puede provocar un evento no deseable que compromete la seguridad del sistema.

Taller

De acuerdo a la definición, busque el concepto en la parte derecha.

1. Tiene como objetivo primario proteger las infraestructuras tecnológicas y de comunicación que soportan la operación de una organización
2. La existencia de una debilidad de diseño, ejecución o error que puede conducir a un acontecimiento inesperado.
3. Se refiere a la privacidad de los elementos de información almacenados y procesados en un sistema informático.
4. Es un estado de confianza personal
5. Es un activo que como otros activos importantes tiene valor y requiere en consecuencia una protección adecuada

Seguridad

Seguridad Informática

Seguridad de la Información

Confidencialidad

Integridad

Información

Amenaza

Vulnerabilidad

Ataque: Proceso de tratar de burlar los controles de seguridad de un sistema o equipo.

Aprovecha toda vulnerabilidad en el software, hardware, e incluso, en las personas que forman parte de un ambiente informático

1. Reconocimiento (Reconnaissance)

En esta fase el atacante crea una estrategia para su ataque. El reconocimiento se refiere a la fase preparatoria donde se obtiene toda la información necesaria antes de lanzar un ataque. Puede incluir Ingeniería Social y Dumpster diving*

**Consiste en buscar papeles o documentos con información confidencial en la basura.*

2. Escaneo (Scanning)

Esta es la fase que un hacker realiza antes de lanzar un ataque a la red. En el escaneo el atacante utiliza toda la información que obtuvo en la Fase 1 para identificar vulnerabilidades específicas.

EJ: Vulnerabilidades OSx

3. Obtener Acceso (Gaining Access)

Esta es una de las fases más importantes para un hacker porque es la fase de penetración al sistema informático, en esta fase un hacker explota las vulnerabilidades que encontró en la fase 2. Ej: Buffer overflows[1], Sesión hijacking[2]

[1] Desbordamiento de búfer

[2] Consigue el identificador de **sesión** entre una página web y un usuario

4. Mantener el Acceso ganado (Maintaining Access)

Una vez que un hacker gana el acceso a un sistema informático (Fase 3) su prioridad es mantener ese acceso que ganó. En esta fase el hacker utiliza recursos propios y los recursos del sistema informático. Además, usa el sistema informático atacado como plataforma de lanzamiento de nuevos ataques informáticos para escanear y explotar a otros sistemas informáticos que pretende atacar. Ej: Sniffers [3]

[3] Es un programa informático que registra la información que envían los periféricos, así como la actividad realizada en un determinado ordenador

5. Cubrir las huellas (Covering Tracks)

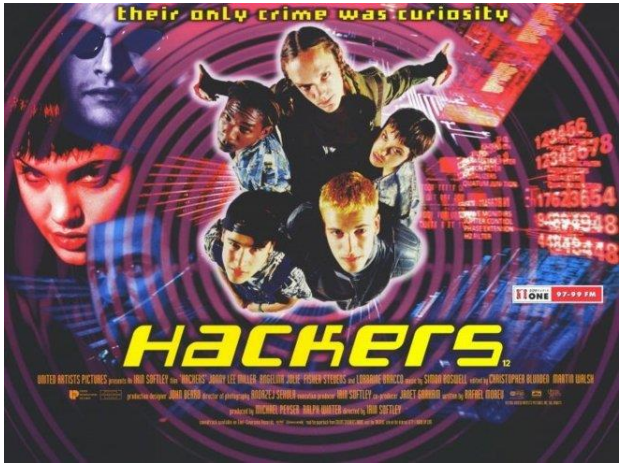
En esta fase es donde un hacker trata de destruir toda evidencia de cualquier posible rastreo de sus actividades ilícitas y lo hace por varias razones, entre ellas: seguir manteniendo el acceso al sistema informático comprometido, ya que si borra sus huellas los administradores de redes no tendrán pistas claras del atacante y el hacker podrá seguir penetrando el sistema cuando quiera. Además borrando sus huellas evita ser detectado y por tanto, anula la posibilidad de ser atrapado por la policía informática y quedar así al margen del imperio de la ley.

ALGUNAS PELICULAS

Juegos de Guerra (1983)

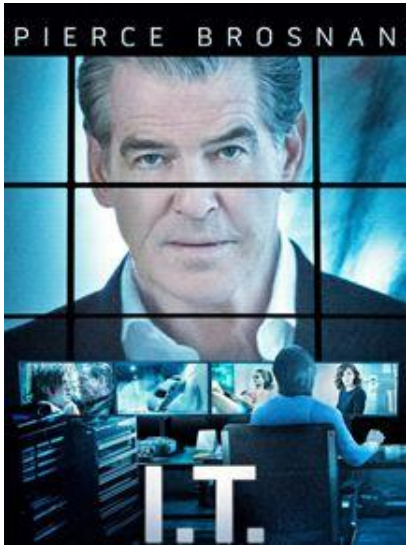
La Red (1995)

Hackers (1995)



Swordfish: Acceso

I.T. (2016)



El circulo (2017)