Implantación de mecanismos de seguridad activa.

UT02 – Seguridad y Alta Disponibilidad

Mari Loli Paralera Romero

IES AL –ÁNDALUS, 23 marzo de 2022

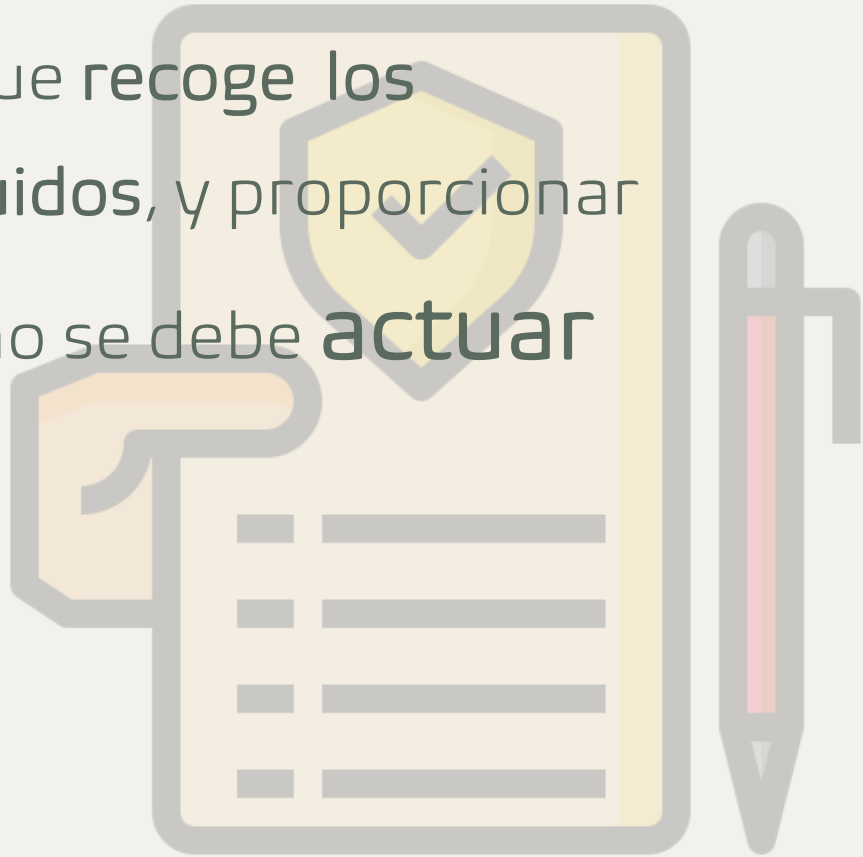
Índice

Plan de Contingencias

1.1

¿Qué es un manual de seguridad?

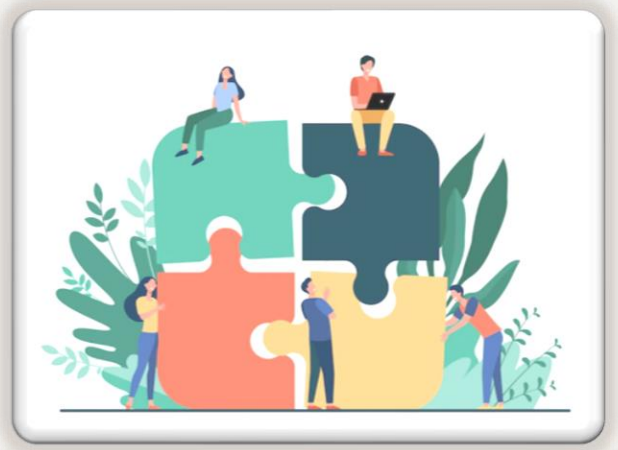
Un manual de seguridad es un documento que **recoge los estándares de seguridad que deben ser seguidos**, y proporcionar un conjunto de normas que determinen como se debe **actuar para evitar problemas.**



¿Qué es un manual de seguridad?

Los pasos para elaborar un manual de seguridad deben ser al menos:

- Formar un equipo integrado por personas de diferentes departamentos de la organización.



¿Qué es un manual de seguridad?

Los pasos para elaborar un manual de seguridad deben ser al menos:

- ❑ Formar un equipo integrado por personas de diferentes departamentos de la organización.
- ❑ Elaborar el documento.
  - Los factores humanos.
  - Los factores tecnológicos.
  - La legislación vigente.
  - Los criterios que determinen la responsabilidad de cada usuario.
  - Los criterios de actuación.

¿Qué es un manual de seguridad?

Los pasos para elaborar un manual de seguridad deben ser al menos:

- ❑ Formar un equipo integrado por personas de diferentes departamentos de la organización.
- ❑ Elaborar el documento.
- ❑ Publicar de manera oficial el manual.

¿Qué es un plan de contingencia?

Es un conjunto de procedimientos que nos van a permitir a **reducir el impacto** de un determinado **imprevisto** dentro de la actividad habitual que se desempeña en la empresa con el objetivo de garantizar su continuidad.

¿Qué es un plan de contingencia?

Es un conjunto de procedimientos que nos van a permitir a **reducir el impacto** de un determinado **imprevisto** dentro de la actividad habitual que se desempeña en la empresa con el objetivo de garantizar su continuidad.

Debe contemplar:

- **Un análisis de riesgos del sistema**.

¿Qué es un plan de contingencia?

Es un conjunto de procedimientos que nos van a permitir a **reducir el impacto** de un determinado **imprevisto** dentro de la actividad habitual que se desempeña en la empresa con el objetivo de garantizar su continuidad.

Debe contemplar:

- ❑ Un análisis de riesgos del sistema.
- ❑ **Un estudio de las protecciones actuales**.

¿Qué es un plan de contingencia?

Es un conjunto de procedimientos que nos van a permitir a **reducir el impacto** de un determinado **imprevisto** dentro de la actividad habitual que se desempeña en la empresa con el objetivo de garantizar su continuidad.

Debe contemplar:

- ❑ Un análisis de riesgos del sistema.
- ❑ Un estudio de las protecciones actuales.
- ❑ **Un plan de recuperación antes, durante y después del desastre**.

¿Qué es un plan de contingencia?

El plan debe **ser dinámico y flexible**, que permita modificaciones frente a **nuevas incidencias** que se pudieran producir a lo **largo del tiempo.**

Etapas Plan de Contingencia

- Evaluación
- Planificación
- Viabilidad
- Ejecución
- Recuperación

¿Qué es un plan de contingencia?

El plan debe **ser dinámico y flexible**, que permita modificaciones frente a **nuevas incidencias** que se pudieran producir a lo **largo del tiempo.**

Etapas Preventivas

- Evaluación
- Planificación
- Viabilidad
- Ejecución
- Recuperación

¿Qué es un plan de contingencia?

El plan debe **ser dinámico y flexible**, que permita modificaciones frente a **nuevas incidencias** que se pudieran producir a lo **largo del tiempo.**

Etapas Paliativas

- Evaluación
- Planificación
- Viabilidad
- Ejecución
- Recuperación

Evaluación - Planificación - Viabilidad

Ser capaces de responder a las siguientes preguntas:

- ¿Qué se debe de proteger?
- ¿Qué puede ir mal?
- ¿Con que frecuencia?
- ¿Cuáles pueden ser las consecuencias?

Debemos conocer que **actividades son prioritarias**, cuantificar **los recursos necesarios**(humanos, materiales y económicos.)

Ejecución - Recuperación

Tener controlado:

- El origen del fallo
- El daño ocasionado
- Cumplir con los procedimientos tal y como se especifican.

Según el desastre ocurrido se pueden clasificar el plan de recuperación en:

Plan de respaldo: Antes

Plan de Emergencia: Durante

Plan de recuperación: Después.

Pautas y Prácticas Seguras

1.2

Las organizaciones gastan millones de dólares en firewalls y dispositivos de seguridad, pero tiran el dinero porque ninguna de estas medidas cubre el eslabón más débil de la cadena de seguridad: la gente que usa y administra los ordenadores.

Kevin Mitnick (El hacker más famoso de todos los tiempos)

Pautas

- Mantener actualizado el sistema operativo y las aplicaciones.
- Descargar software desde sitios de confianza, especialmente las actualizaciones de los sistemas operativos.
- Analizar los sistemas de manera periódica para mantenerlos libres de software malicioso.
- Usar contraseñas robustas siguiendo las pautas de acuerdo a una buena política de contraseñas.
- Usar certificados digitales.
- Comunicar las incidencias.
- Realizar copias de seguridad.

Pautas

- Creer que el software de seguridad es 100% efectivo.
- Pensar que algún equipo no debe protegerse porque no almacena nada importante.
- Creer que los ataques informáticos solamente los sufren personas u organizaciones importantes.

Herramientas preventivas / paliativas

Tratan **de evitar que un sistema sea atacado** y prevenir las amenazas (Confidencialidad, Integridad, Disponibilidad, Autenticación y No repudio) de los elementos críticos de un sistema.

Tienen como objetivo **minimizar el impacto** producido por un ataque.

Herramientas preventivas / paliativas

La **actualización de sistemas** y aplicaciones quizás sea una de las medidas, más adecuadas para **prevenir daños en los sistemas informáticos.**

Todos los sistemas tienen fallos de seguridad y a medida que surgen nuevas aplicaciones y técnicas, pueden surgir más vulnerabilidades.

- ✓ Corregir fallos detectados.
- ✓ Añadir nuevas funcionalidades.

Herramientas Preventivas

- Instalación de software **antimalware**.
- Configuración adecuada de **cortafuegos**.
- Encriptación de la información usando **comunicaciones SSL**.
- Instalación de herramientas de **detección de intrusos**.
- Utilización de mecanismos de **autenticación**.
- Utilización de **sistemas tolerantes a fallos**.
- Utilización segura de entornos físicos para protegerse ante incendios, inundaciones,...
- Instalación de sistemas de climatización y de sistemas de alimentación ininterrumpida.

Herramientas Paliativas

- Copias de respaldo o backup.
- Buena política de copias
- Sistemas de discos independientes (RAID)
- Uso de Cloud Computing – copias en la nube

QNAP

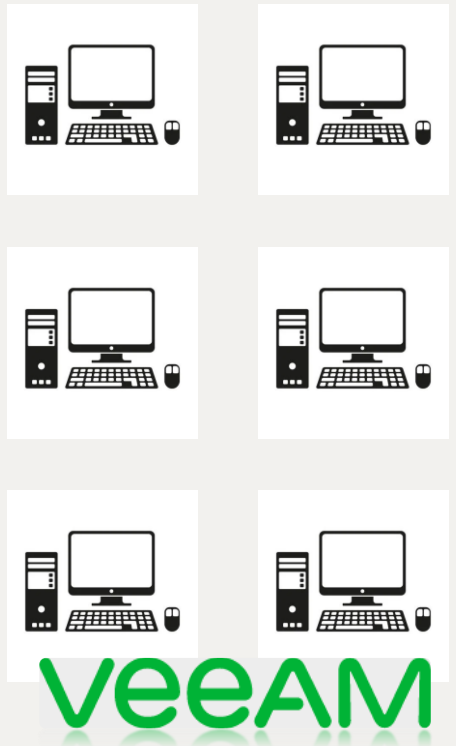
IBM Cloud

VEEAM

Ejemplo de sistema de copias

Veeam Servidor

IP de los agentes
Trabajos creados de cada agente



<u>Recuperación completa</u>

Veeam Recovery Media:

- Imagen de recuperación de arranque
- Copia de seguridad del equipo cuyos datos desea restaurar

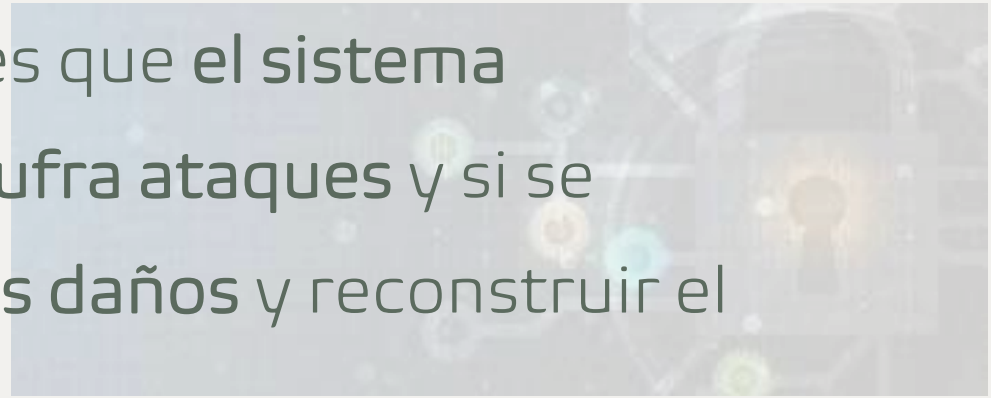
Veamos recomendaciones de buenas prácticas

Ataques y contramedidas en sistemas personales.

02

Ataques y contramedidas en sistemas personales.

El **objetivo** de **la seguridad** de un sistema es que **el sistema permanezca en condiciones optimas**, **no sufra ataques** y si se llevan a cabo dichos ataques, **minimizar los daños** y reconstruir el sistema lo antes posible.



Ataques y contramedidas en sistemas personales.

El **objetivo** de **la seguridad** de un sistema es que **el sistema permanezca en condiciones optimas**, **no sufra ataques** y si se llevan a cabo dichos ataques, **minimizar los daños** y reconstruir el sistema lo antes posible.

Ataques y contramedidas en sistemas personales.

Se puede hacer una clasificación de la seguridad como:

FL Seguridad Física o lógica

AP Seguridad Activa o pasiva.

Seguridad Física

La **seguridad física** de un sistema informático consiste en la aplicación de barreras físicas y procedimientos de control frente **a amenazas físicas al hardware**.

Seguridad Lógica

La seguridad lógica de un sistema informático consiste en la **aplicación de barreras** y procedimientos que **protejan el acceso a los datos** y al **información contenida en él.**

Ataques y contramedidas en sistemas personales.

Estas amenazas, tanto físicas como lógicas, son materializadas básicamente por:

FL Física o lógica

Las personas

Ataques y contramedidas en sistemas personales.

Estas amenazas, tanto físicas como lógicas, son materializadas básicamente por:

FL Física o lógica

Las personas

Programas

Ataques y contramedidas en sistemas personales.

Estas amenazas, tanto físicas como lógicas, son materializadas básicamente por:

FL Física o lógica

Las personas

Programas

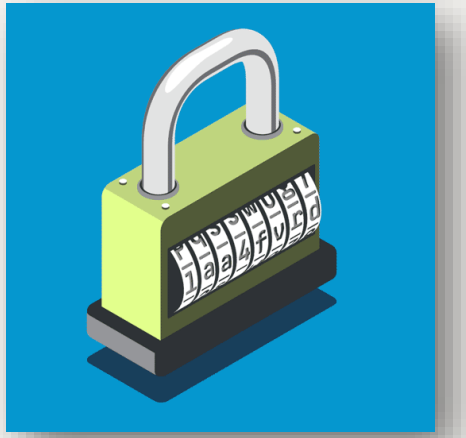
Catástrofes

Seguridad Activa

Se dice que se emplean **mecanismos de seguridad** activa cuando estos tienen como objetivo **evitar daños en el sistema**.

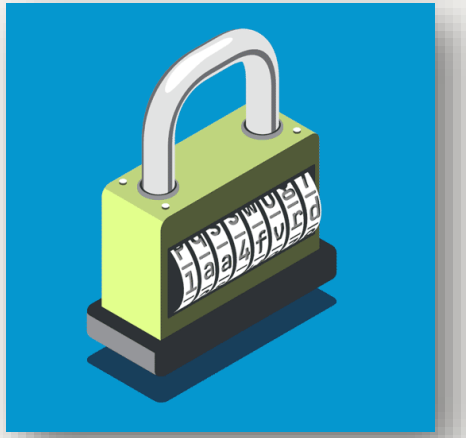
Seguridad Activa

Se dice que se emplean **mecanismos de seguridad** activa cuando estos tienen como objetivo **evitar daños en el sistema.**



Seguridad Activa

Se dice que se emplean **mecanismos de seguridad** activa cuando estos tienen como objetivo **evitar daños en el sistema.**



Seguridad Pasiva

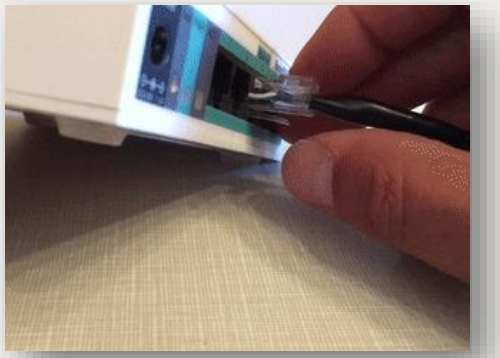
Se dice que se emplean **mecanismos de seguridad** pasiva cuando estos se emplean para **minimizar los daños causados por un incidente de seguridad**.

Seguridad Pasiva

Se dice que se emplean **mecanismos de seguridad** pasiva cuando estos se emplean para **minimizar los daños causados por un incidente de seguridad**.

Seguridad Pasiva

Se dice que se emplean **mecanismos de seguridad** pasiva cuando estos se emplean para **minimizar los daños causados por un incidente de seguridad**.



La diferencia entre seguridad activa y pasiva es que:

A La seguridad activa es lógica y la pasiva física.

B La activa se emplea para evitar daños y la pasiva para minimizarlos.

C No hay diferencia, de hecho hay aplicaciones que se utilizan tanto para prevenir como para paliar.

D La activa minimiza los daños y la pasiva previene.

La diferencia entre seguridad activa y pasiva es que:

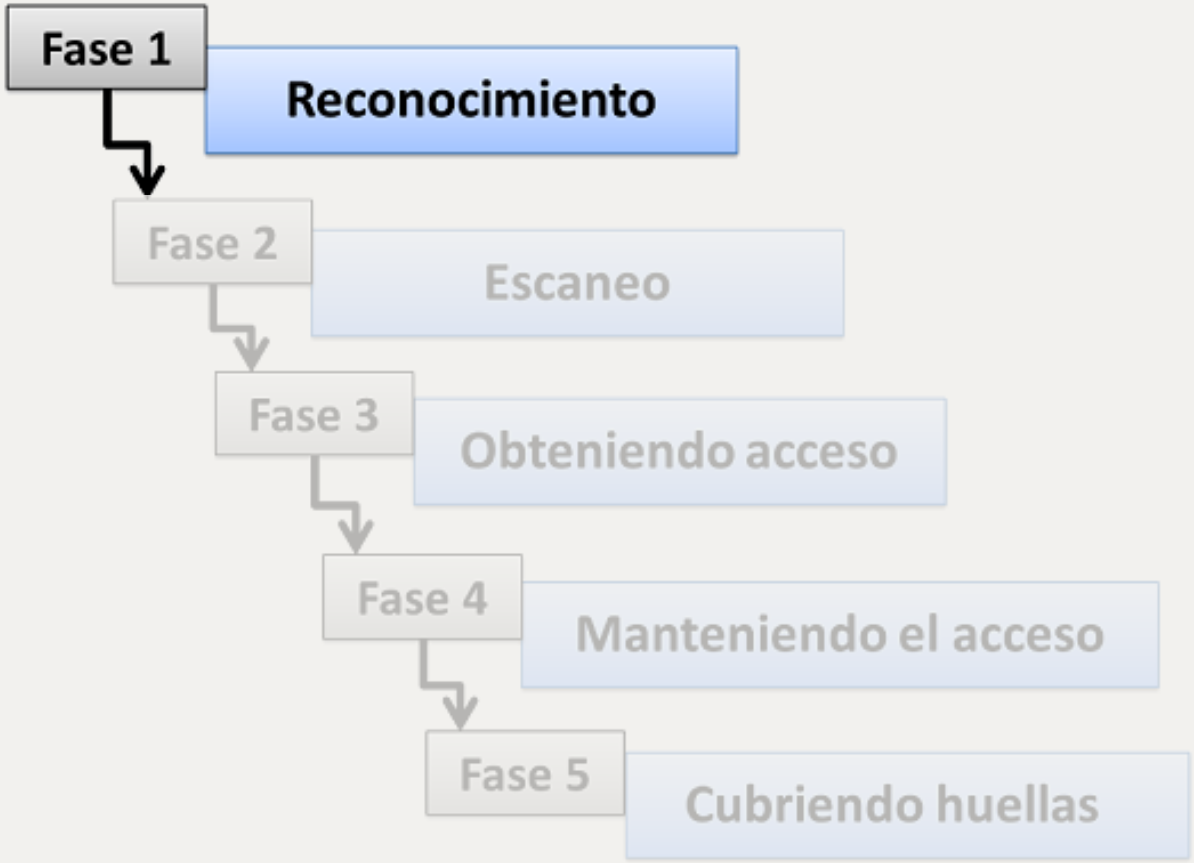
A La seguridad activa es lógica y la pasiva física.

B La activa se emplea para evitar daños y la pasiva para minimizarlos.

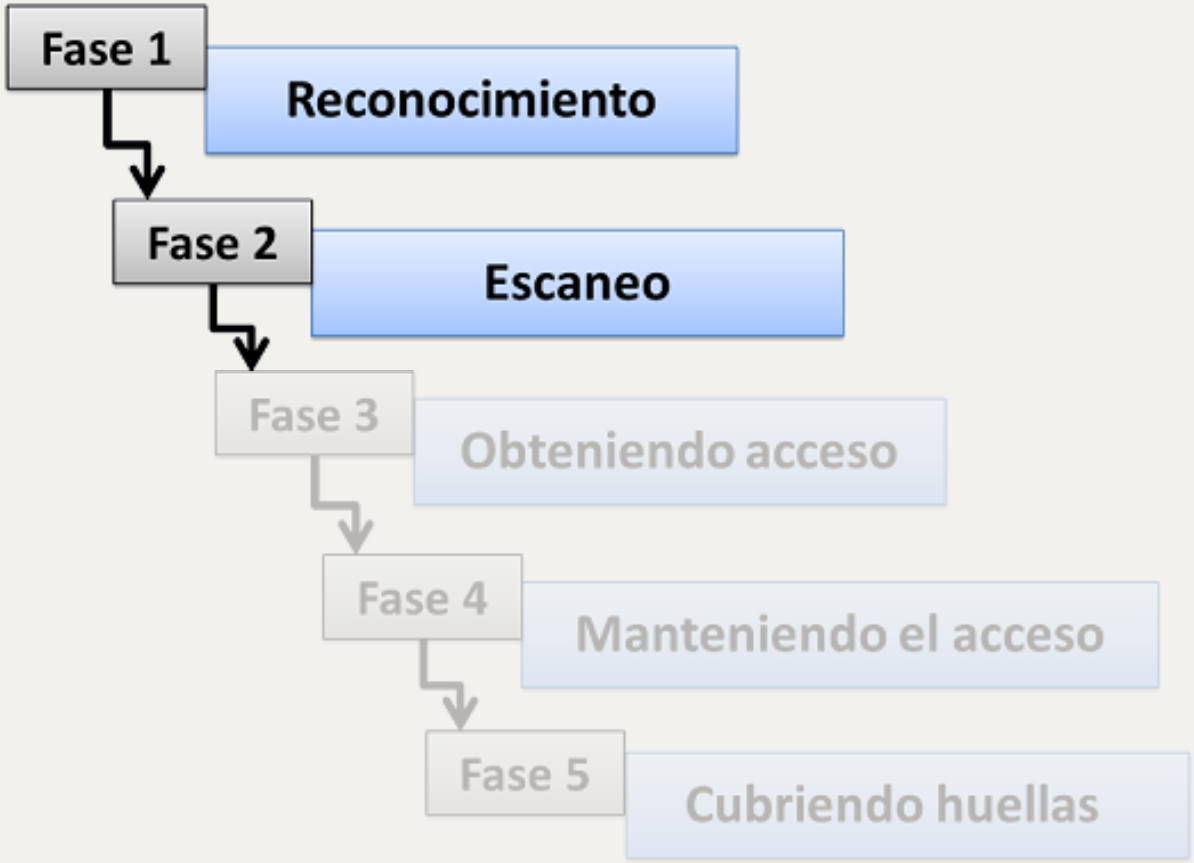
C No hay diferencia, de hecho hay aplicaciones que se utilizan tanto para prevenir como para paliar.

D La activa minimiza los daños y la pasiva previene.

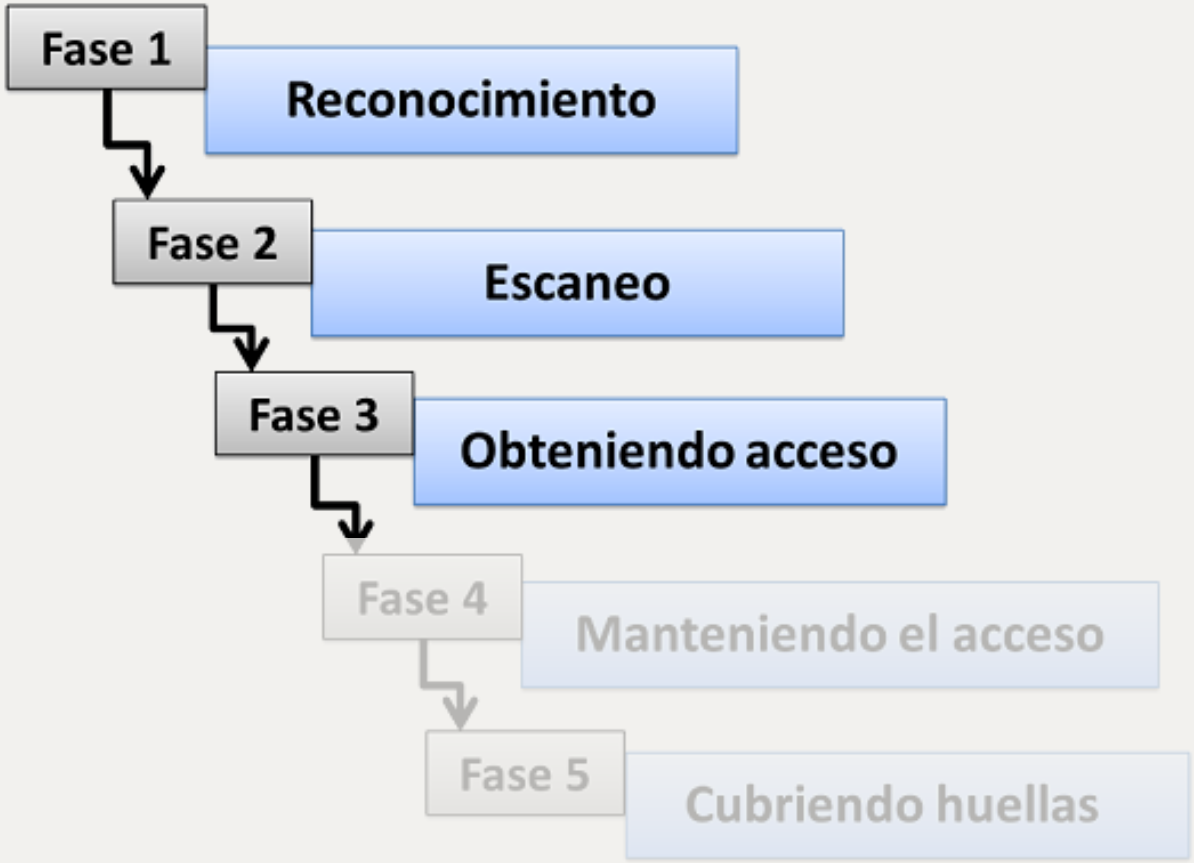
Fases de un ataque informático



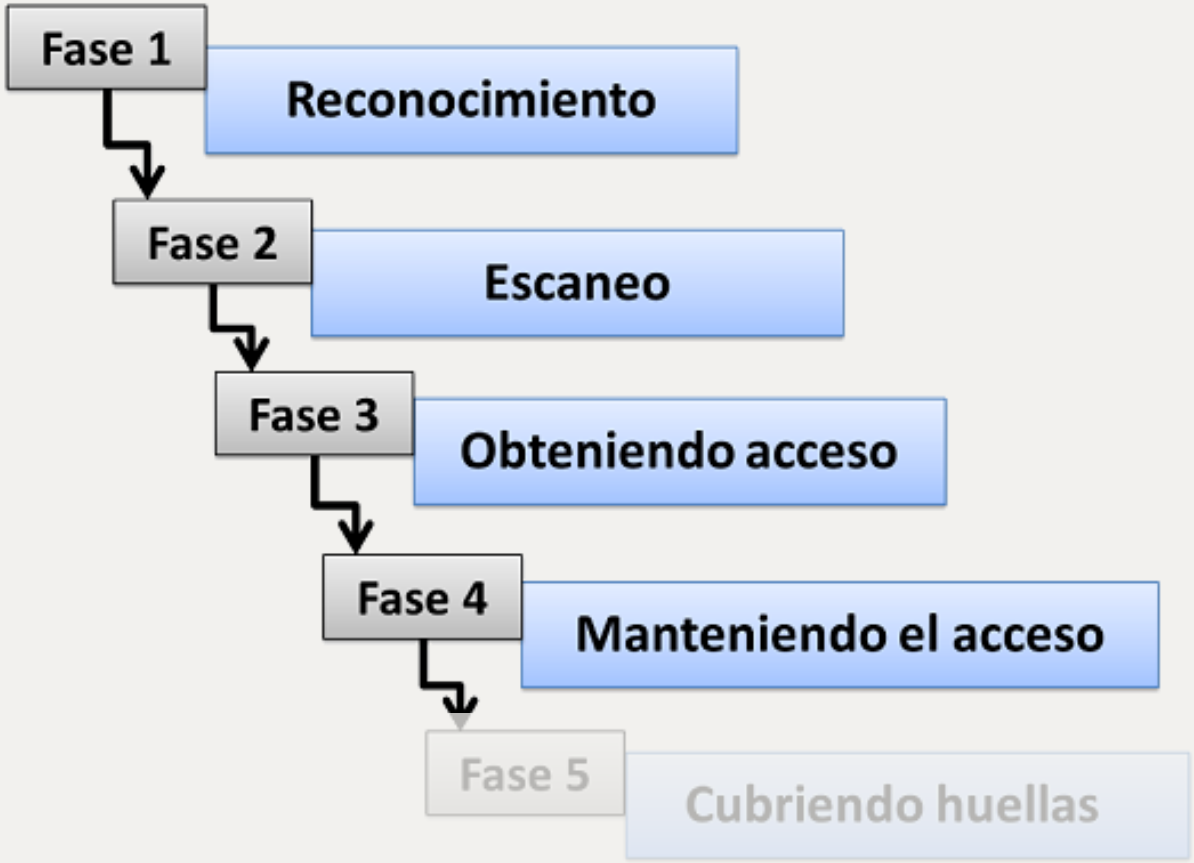
Fases de un ataque informático



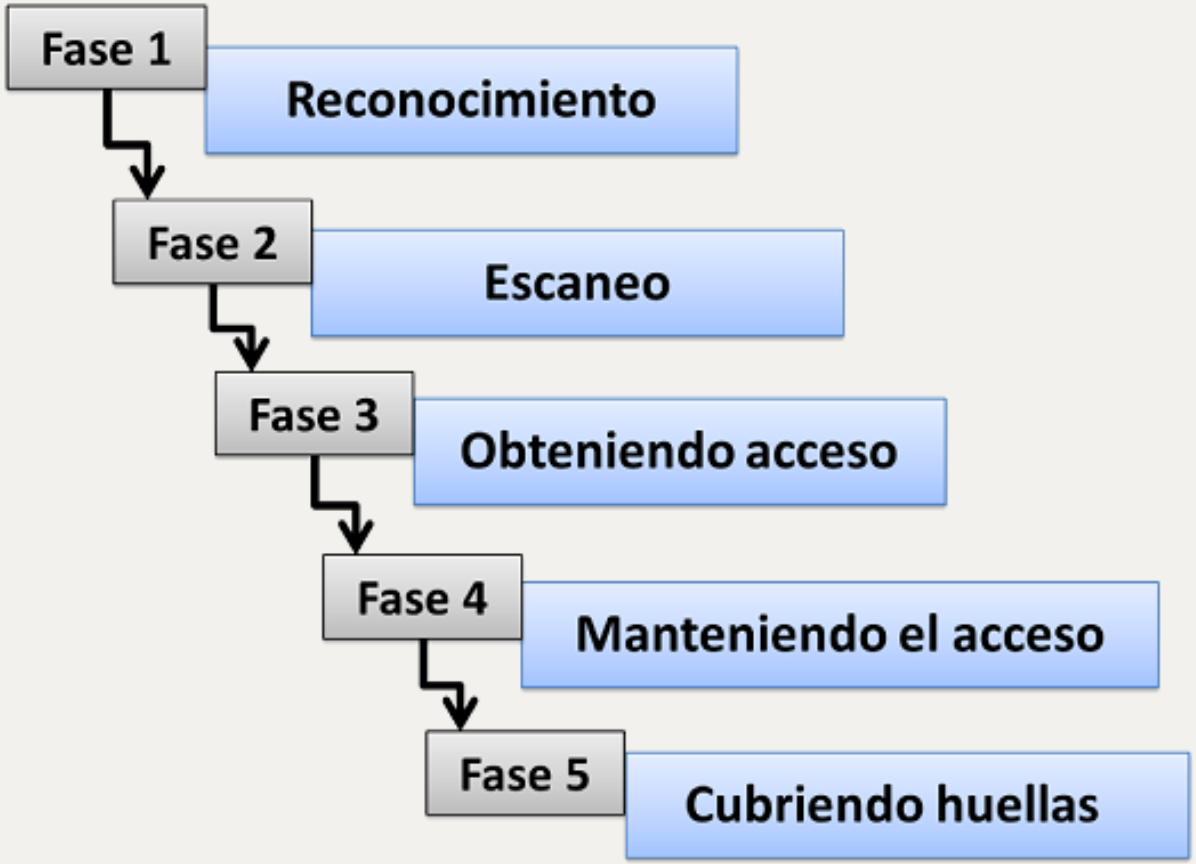
Fases de un ataque informático



Fases de un ataque informático



Fases de un ataque informático



Clasificación de los ataques

Ataques Pasivos

No producen cambios, se limitan a extraer información y en la mayoría de los casos el afectado no percibe el ataque.

Ataques Activos

En cambio, los ataques activos **producen cambios** en el sistema

Clasificación de los ataques

Ataques Pasivos

- Lecturas de las cabeceras de los paquetes monitorizados.
- Control del volumen de tráfico intercambiado entre las entidades monitorizadas
- Control de las horas habituales de intercambio de datos

Clasificación de los ataques

Ataques Pasivos

- Lecturas de las cabeceras de los paquetes monitorizados.
- Control del volumen de tráfico intercambiado entre las entidades monitorizadas
- Control de las horas habituales de intercambio de datos

Ataques Activos

- Suplantación de identidad
- Modificación de mensajes
- Degradación fraudulenta del servicio

Un ataque se clasifica como activo o pasivo:

A Tomando como criterio el efecto que produce en el sistema.

B Dependiendo del tipo de seguridad que tenga el sistema.

C Dependiendo del tiempo en el que se produce.

D Si roba información o no.

Un ataque se clasifica como activo o pasivo:

A Tomando como criterio el efecto que produce en el sistema.

B Dependiendo del tipo de seguridad que tenga el sistema.

C Dependiendo del tiempo en el que se produce.

D Si roba información o no.

Clasificación de los ataques

Tipos de ataques

- **Reconocimiento de sistemas** (footprinting o information gathering).

Es la técnica utilizada para recopilar información sobre los sistemas informáticos y las entidades a las que pertenecen

Veamos varios ejemplos:

SHODAN


Héctor Rizaldos
¿QUÉ ES SHODAN
Y PARA QUÉ USARLO?

Veamos varios ejemplos:


HACKING CON
Google

Clasificación de los ataques

Tipos de ataques

- Reconocimiento de sistemas (footprinting o information gathering).
- Explotación de las **vulnerabilidades del sistema**.
- Robo de información por interceptación de mensajes.
- Inyección de código SQL.

Los ataques que aprovechan las vulnerabilidades del sistema se basan en programas que se diseñan de manera específica para aprovechar una determinada vulnerabilidad.

Estos programas reciben el nombre de **exploits**.

Clasificación de los ataques

Tipos de ataques

- Reconocimiento de sistemas (footprinting o information gathering).
- Explotación de las vulnerabilidades del sistema.
- Robo de información por **interceptación de mensajes.**
- Suplantación de identidad.
- Modificación de información.
- Cross Site Scripting.
- Inyección de código SQL.
- Contra usuarios y contraseñas.

Es un tipo de ataque que tiene como objetivo el robo de información

Clasificación de los ataques

Tipos de ataques

- Reconocimiento de sistemas (footprinting o information gathering).
- Explotación de las vulnerabilidades del sistema.
- Robo de información por **interceptación de mensajes.**
- Suplantación de identidad.
- Modificación de información.
- Denegación de servicio.
- Inyección de código.
- Contra usuarios.

Es un tipo de ataque que tiene como objetivo el robo de información

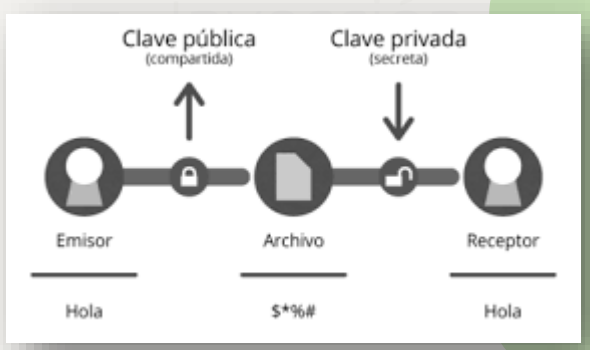
Una solución es encriptar la información, por ejemplo, usando con **PGP** o S\MIME.

Clasificación de los ataques

Tipos de ataques

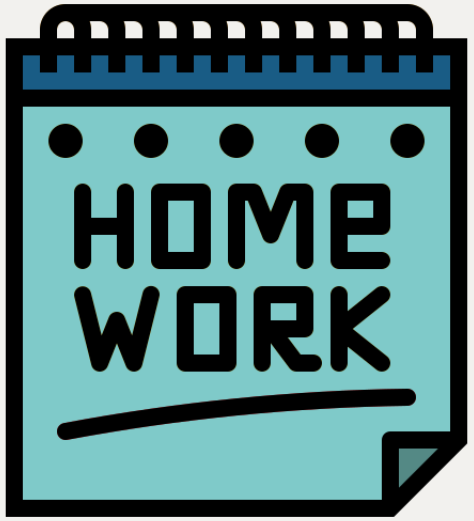
- Reconocimiento de sistemas (footprinting o information gathering).
- Explotación de las vulnerabilidades del sistema.
- Robo de información por **interceptación de mensajes.**
- Suplantación de identidad.

Es un tipo de ataque que tiene como objetivo el robo de información



Una solución es encriptar la información, por ejemplo, usando con **PGP** o S\MIME.

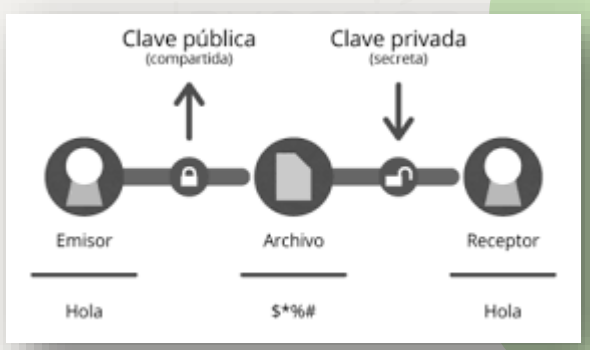
Clasificación de los ataques



Tipos de ataques

- Reconocimiento de sistemas (footprinting o information gathering).
- Explotación de las vulnerabilidades del sistema.
- Robo de información por **interceptación de mensajes.**
- Suplantación de identidad.

Es un tipo de ataque que tiene como objetivo el robo de información



Una solución es encriptar la información, por ejemplo, usando con **PGP** o S\MIME.

Clasificación de los ataques

Tipos de ataques

- Reconocimiento de sistemas (footprinting o information gathering).
- Explotación de las vulnerabilidades del sistema.
- Robo de información por **interceptación de mensajes**.
- **Suplantación de identidad**.

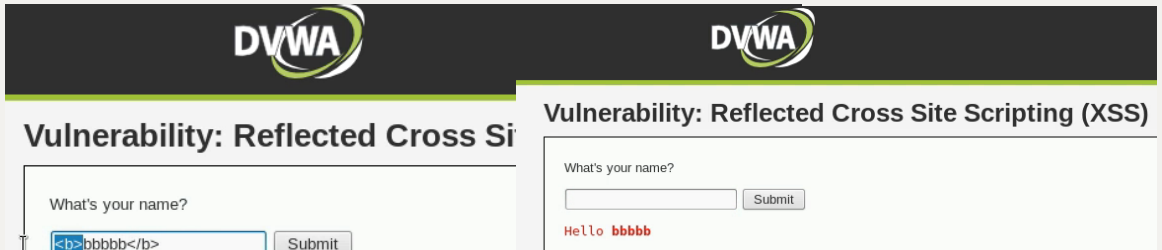
Se enmascaran las direcciones **MAC** (ARP Spoofing)
Se enmascaran las direcciones **IP** (IP Spoofing).
Se produce una **traducción falsa de los servidores DNS** (DNS Spoofing).
Se produce un envío de **mensajes con remitentes falsos** (SMTP Spoofing).
Se **capturan** nombres de **usuario o contraseñas**.

Clasificación de los ataques

Tipos de ataques

- Reconocimiento de sistemas (footprinting o information gathering).
- Explotación de las vulnerabilidades del sistema.
- Robo de información por **interceptación de mensajes**.
- Suplantación de identidad.
- **Cross-site Scripting.**

También llamado **XSS** es un tipo de ataque en el cual actores maliciosos logran **inyectar un script malicioso** en un sitio web para luego ser procesado y ejecutado.



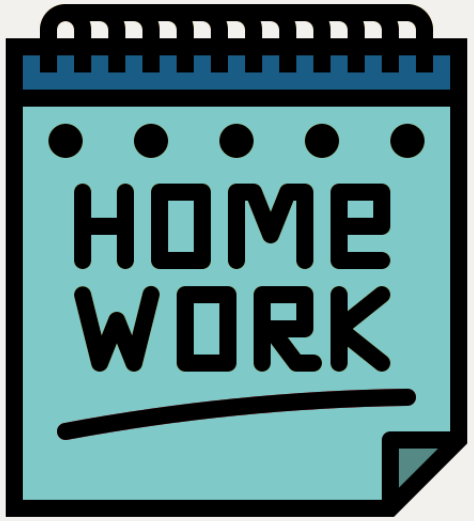
Clasificación de los ataques

Tipos de ataques

- Reconocimiento de sistemas (footprinting o information gathering).
- Explotación de las vulnerabilidades del sistema.
- Robo de información por **interceptación de mensajes**.
- Suplantación de identidad.
- Cross-site Scripting.
- **Inyección de código SQL.**

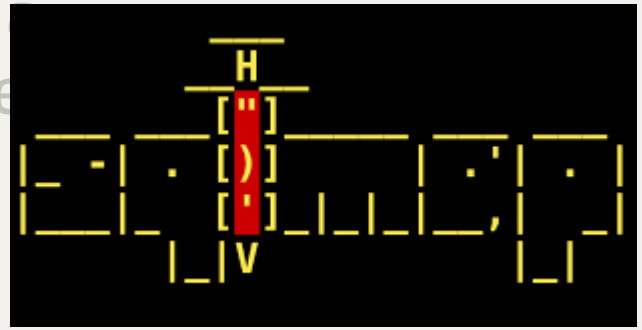
Inyección SQL es un método de infiltración de código intruso que se vale de una vulnerabilidad informática presente en una aplicación en el nivel de validación de las entradas para realizar operaciones sobre una base de datos.

Clasificación de los ataques



Tipos de ataques

- Reconocimiento de sistemas (footprinting o information gathering).
- Explotación de las vulnerabilidades del sistem
- Robo de información por **interceptación de me**
- Suplantación de identidad.
- Cross-site Scripting.
- **Inyección de código SQL.**



Inyección SQL es un método de infiltración de código intruso que se vale de una vulnerabilidad informática presente en una aplicación en el nivel de validación de las entradas para realizar operaciones sobre una base de datos.

Clasificación de los ataques

Tipos de ataques

- Reconocimiento de sistemas (footprinting o information gathering).
- Explotación de las vulnerabilidades del sistema.
- Robo de información por **interceptación de mensajes**.
- Suplantación de identidad.
- Cross-site Scripting.
- Inyección de código SQL.
- **Contra usuarios y contraseñas.**

Ataques con fuerza bruta o ataques de diccionario cuya finalidad es obtener el acceso al sistema.

Gracias

UT02 – Seguridad y Alta Disponibilidad

Mari Loli Paralera Romero

IES AL –ÁNDALUS, 23 marzo de 2022