Sistemas Operativos

Docente:

Ing. Washington Loza H. Mgs.

Departamento de Ciencias de la Computación

Tercer Parcial

Gestión de Seguridad

Introducción

La seguridad en los sistemas operativos es un pilar fundamental en la protección de la información, ya que estos sistemas administran los recursos de hardware y software.

La gestión de seguridad abarca la protección contra amenazas y software malicioso, la implementación de medidas de seguridad, y la evaluación de la seguridad en diferentes plataformas como Windows, Linux, Android y macOS.

Gestión de Seguridad

Amenazas y Software Malicioso

Las amenazas en sistemas operativos son cualquier evento o ataque que pueda comprometer la integridad, confidencialidad o disponibilidad de los datos.

El software malicioso o **malware** es un tipo de programa diseñado para dañar, explotar o interrumpir el funcionamiento de un sistema.

Gestión de Seguridad

Tipos de Amenazas MALWARE

Malware (Software Malicioso): Programas diseñados para infiltrarse o dañar un sistema.

Virus: Se adjunta a archivos ejecutables y se propaga al ser ejecutado.

Gusanos: Se replican automáticamente sin intervención del usuario.

Troyanos: Se disfrazan de programas legítimos para obtener acceso no autorizado.

Ransomware: Bloquea el acceso a los archivos del usuario y exige un rescate para desbloquearlos.

Spyware: Recoge información del usuario sin su consentimiento.

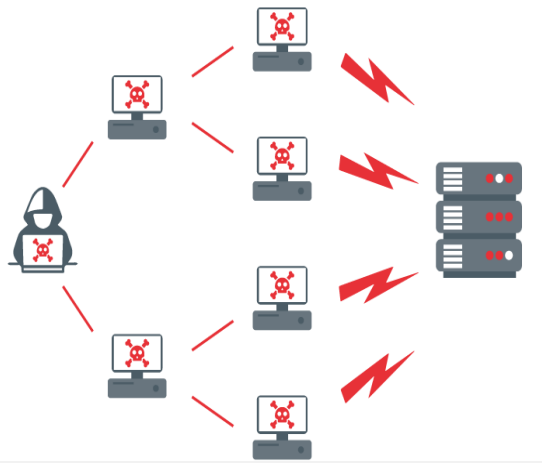
Gestión de Seguridad

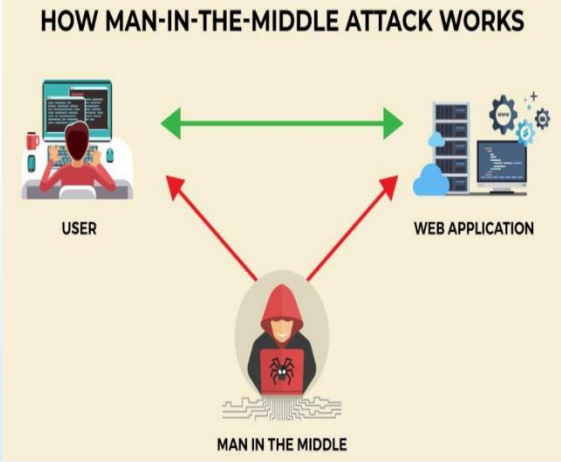
Tipos de Amenazas ATAQUES DE RED

Denegación de Servicio (DoS/DDoS): Sobrecarga un sistema hasta que deja de responder.

Phishing: Engaño para obtener credenciales del usuario.

Man-in-the-Middle (MITM): Intercepción de datos entre dos partes sin que lo sepan.



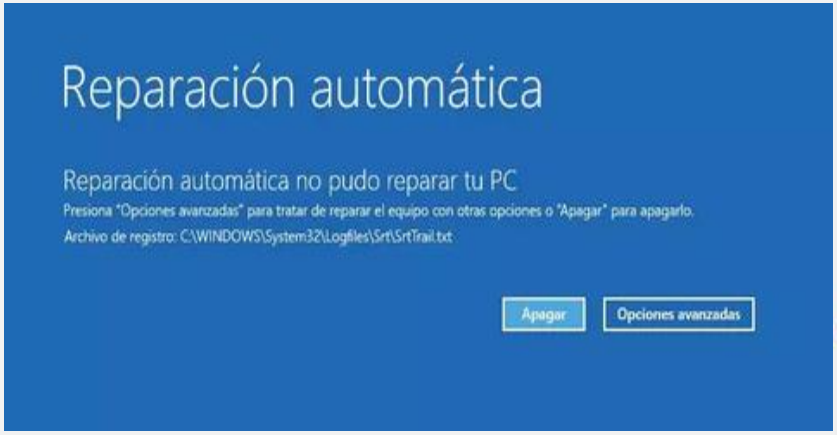


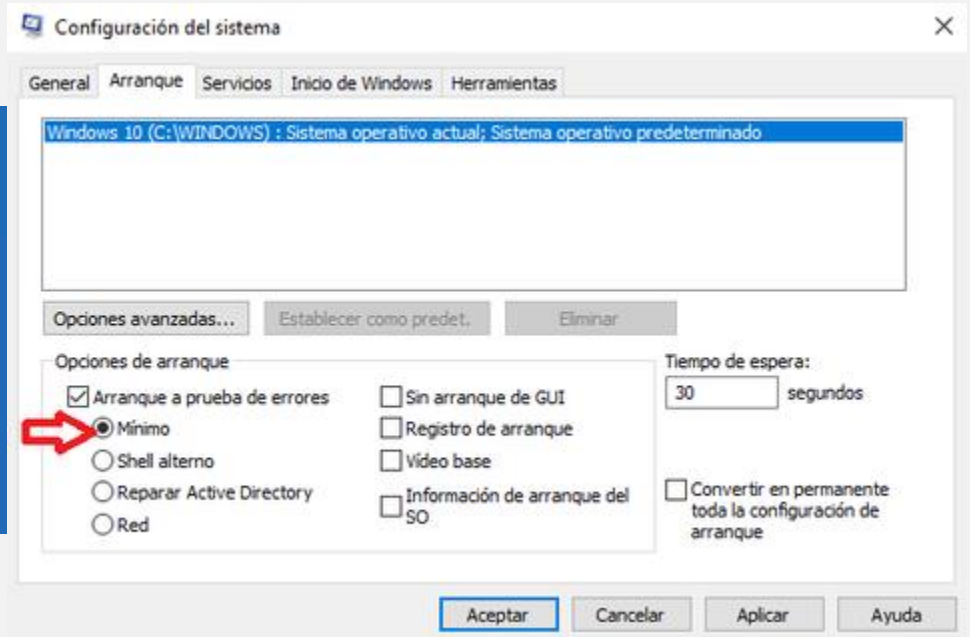
Gestión de Seguridad

Tipos de Amenazas Exploits y Vulnerabilidades

Aprovechan fallos en el software para obtener acceso no autorizado.

Ejemplo: Ataques Zero-Day (fallos desconocidos sin parches disponibles).





Gestión de Seguridad

Medidas de Seguridad y Protección

Para mitigar las amenazas y ataques, es crucial implementar estrategias de seguridad adecuadas.

Autenticación Segura

- Uso de contraseñas robustas y autenticación multifactor (MFA).
- Implementación de sistemas biométricos.

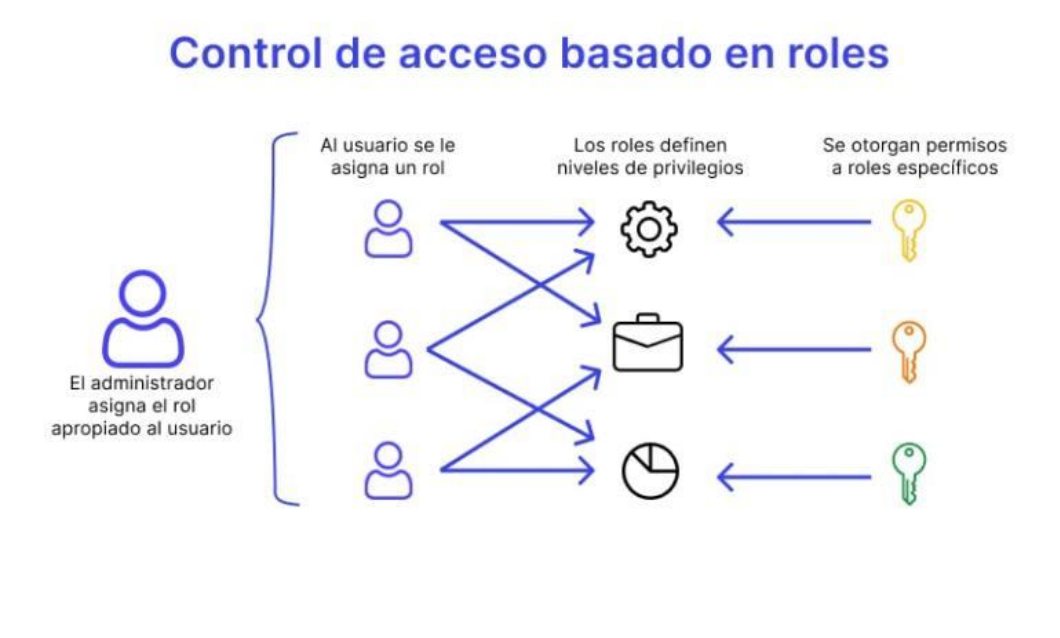
FUENTE: https://fastercapital.com/es/tema/autenticaci%C3%B3n-multifactor-%28mfa%29-para-seguridad-mejorada.html

Gestión de Seguridad

Medidas de Seguridad y Protección ACL

Control de Acceso

- Permisos y roles bien definidos (Usuarios, Administradores, Invitados).
- Uso de listas de control de acceso (ACLs).

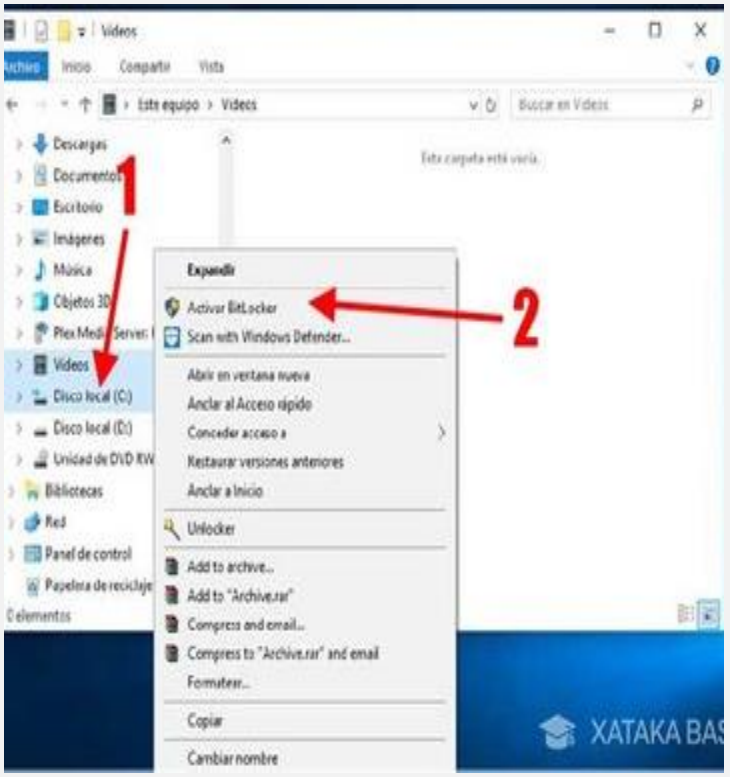


Gestión de Seguridad

Medidas de Seguridad y Protección Cifrado de Datos

Cifrado de Datos

- Uso de algoritmos de cifrado como AES y RSA.
- Implementación de discos cifrados con herramientas como BitLocker (Windows) o LUKS (Linux).

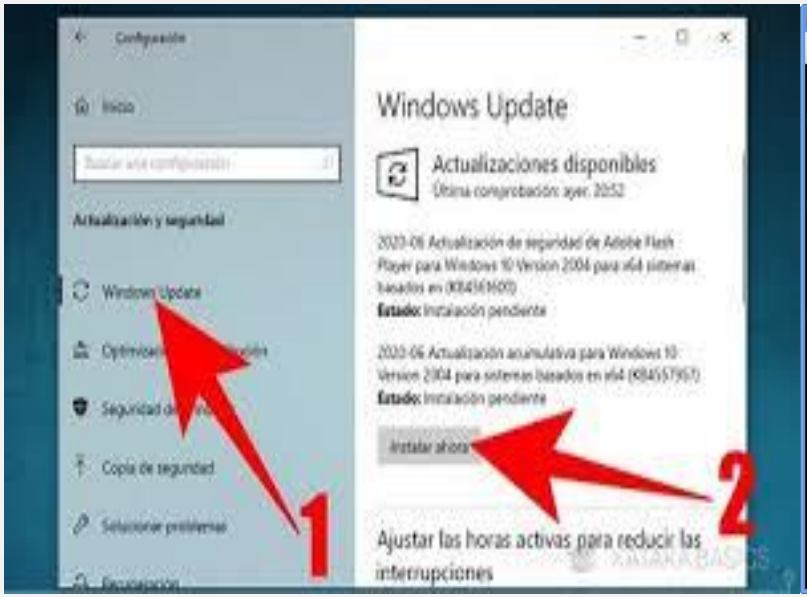


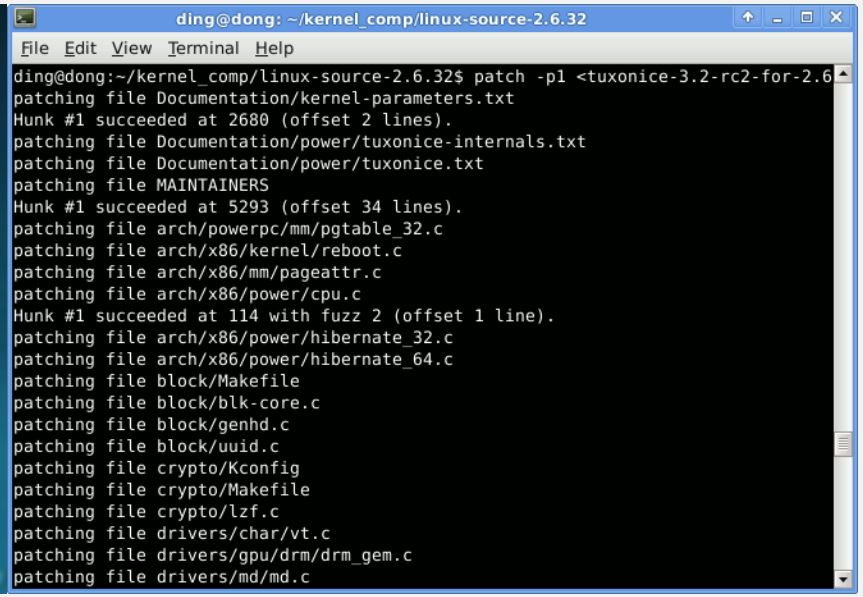
Gestión de Seguridad

Medidas de Seguridad y Protección Parches de Seguridad

Actualización y Parches de Seguridad

- Aplicación de actualizaciones periódicas del sistema operativo y software.
- Uso de herramientas de gestión de vulnerabilidades.



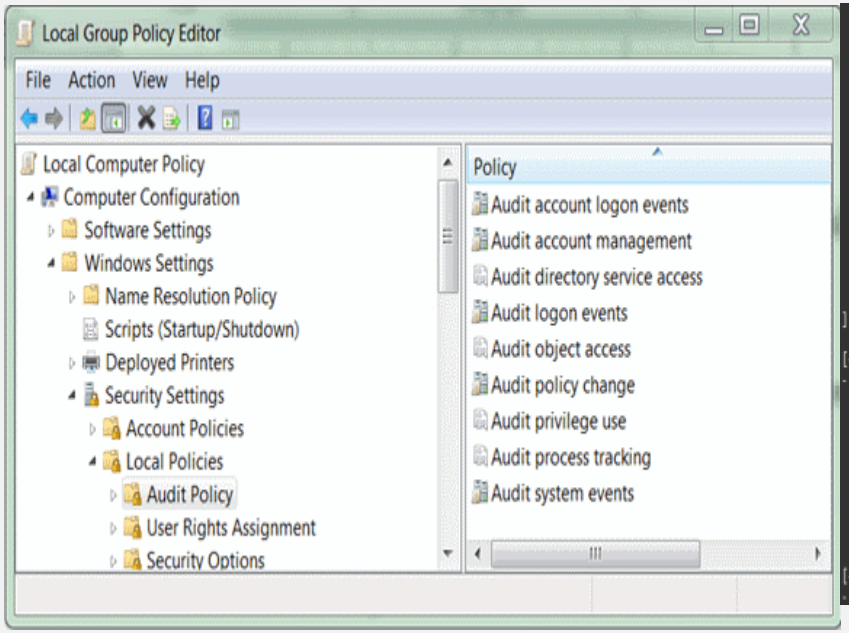


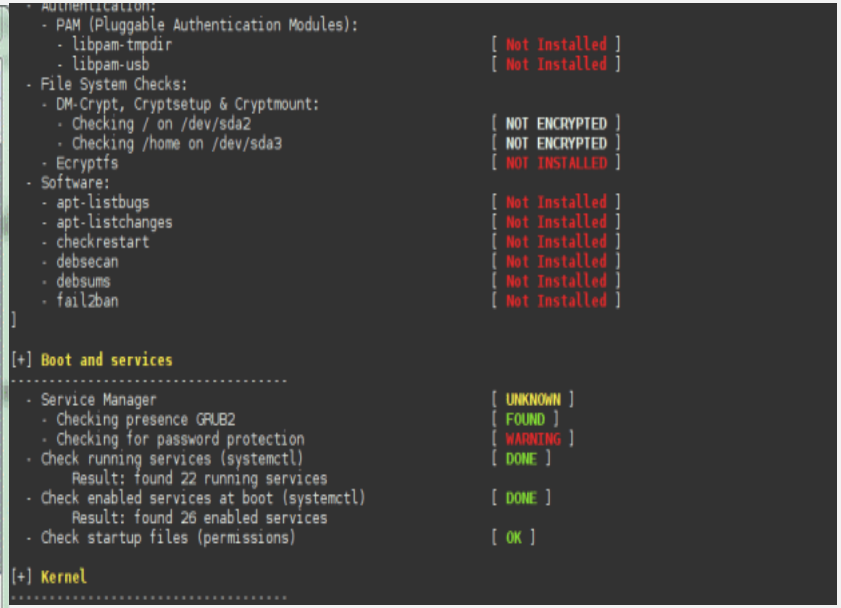
Gestión de Seguridad

Medidas de Seguridad y Protección Monitoreo y Auditoria

Monitoreo y Auditoría

- Uso de herramientas SIEM para análisis de eventos y detección de intrusos.
- Registro de logs y análisis de patrones de tráfico.



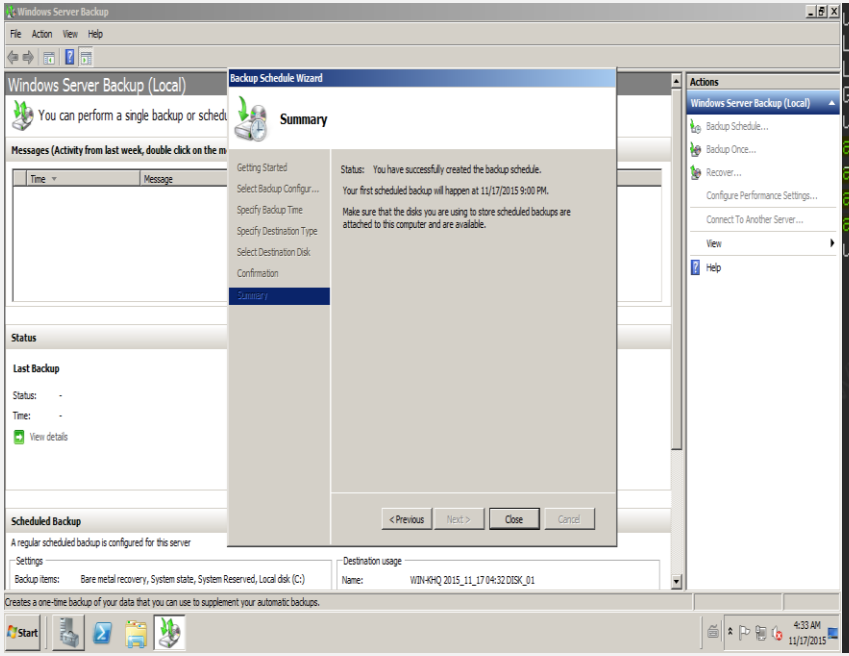


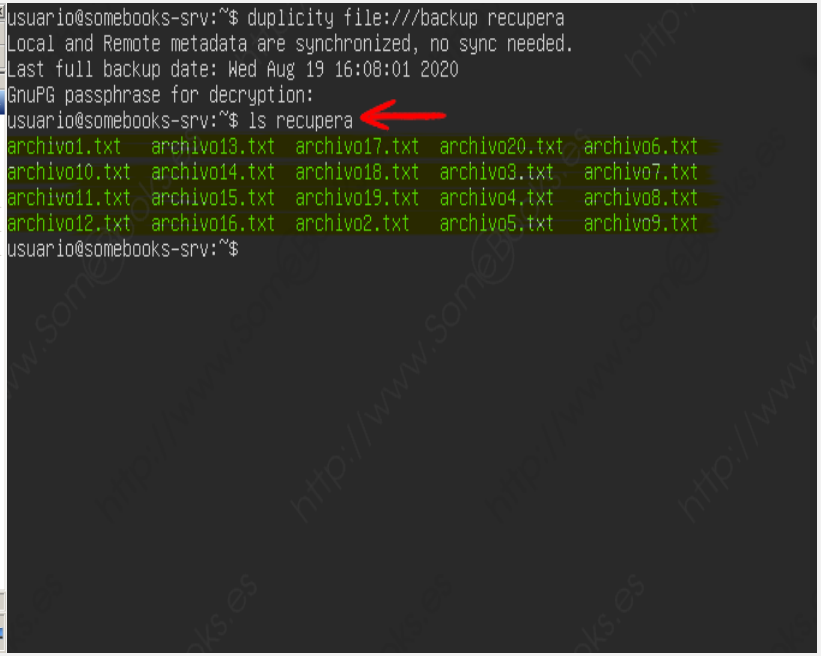
Gestión de Seguridad

Medidas de Seguridad y Protección Resp. Información

Respaldo de Información

- Estrategias de backup en la nube y local (Regla 3-2-1: 3 copias, 2 medios diferentes, 1 externo).





UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

Seguridades de S.O.

- **Trabajo de Investigación:**

Seguridades en diversos Sistemas Operativos (Windows-Linux)

Seguridades para Android y iOS