CENTRO UNIVERSITARIO DE CIENCIAS EXACTAS E INGENIERÍAS (CUCEI)

Departamento de ciencias computacionales

Seminario de solución de problemas de uso, adaptación, explotación de sistemas operativos

Violeta del Rocío Becerra Velázquez

Jose Pedro Reyes Alvarez

222790897

Ingeniería Informática (INNI)

D02

3.3 Seguridad

18 de mayo del 2025

Tabla de contenido

Seguridad y protección en sistemas operativos

La seguridad en un sistema operativo se refiere al conjunto de mecanismos y políticas que permiten proteger la integridad, confidencialidad y disponibilidad de la información y los recursos gestionados por el sistema. El sistema operativo actúa como el intermediario entre el usuario y el hardware, por lo tanto, es el primer nivel de defensa contra amenazas.

Principales aspectos de seguridad

- Control de acceso:
  El sistema operativo debe asegurarse de que solo usuarios autorizados puedan acceder a los recursos del sistema, como archivos, dispositivos o memoria. Esto se logra mediante permisos, autenticación (contraseñas, biometría) y cuentas de usuario.
- Autenticación:
  Es el proceso por el cual se verifica la identidad de un usuario. Los sistemas operativos utilizan diversos métodos, como contraseñas, tokens, tarjetas inteligentes o sistemas biométricos.
- Autorización:
  Una vez autenticado un usuario, el sistema debe determinar qué acciones puede realizar. Por ejemplo, si tiene permiso para leer, escribir o ejecutar un archivo.
- Auditoría y registro (logs):
  El sistema operativo registra las acciones de los usuarios en archivos de log. Esto permite detectar comportamientos sospechosos y rastrear incidentes de seguridad.
- Protección contra malware:
  Muchos sistemas operativos integran herramientas para detectar, bloquear y eliminar software malicioso como virus, troyanos, ransomware y spyware.
- Actualizaciones de seguridad:
  Los desarrolladores de sistemas operativos lanzan actualizaciones periódicas para corregir vulnerabilidades detectadas. Mantener el sistema actualizado es clave para su seguridad.

Ejemplos de seguridad en diferentes sistemas operativos

- Windows: Usa herramientas como Windows Defender, Control de cuentas de usuario (UAC) y BitLocker (cifrado de disco).
- Linux: Utiliza permisos estrictos de archivos, firewalls como iptables, y sistemas de control como SELinux o AppArmor.
- macOS: Ofrece cifrado FileVault, control de apps mediante Gatekeeper y un sistema de aislamiento (sandboxing) para aplicaciones.

Relación con la seguridad en la red

Los sistemas operativos deben estar preparados para proteger al equipo cuando está conectado a una red. Esto incluye:

- Configurar correctamente los firewalls.
- Cifrar las comunicaciones con protocolos como HTTPS o SSH.
- Detectar y bloquear conexiones no autorizadas.
- Gestionar correctamente las políticas de red y el acceso a servicios.

Seguridad y protección en la red

La seguridad en la red se refiere a las políticas, tecnologías y prácticas utilizadas para prevenir el acceso no autorizado, mal uso, modificación o denegación del servicio dentro de una red informática. Su objetivo principal es proteger la información mientras viaja entre dispositivos conectados por una red, ya sea local (LAN) o global como Internet.

Principales amenazas a la red

- Ataques de malware: Virus, troyanos, spyware y ransomware que se propagan a través de la red para dañar o robar información.
- Phishing: Correos o mensajes falsos que engañan a los usuarios para obtener datos personales.
- Ataques DDoS: Sobrecargan servidores con múltiples solicitudes para que el servicio deje de funcionar.
- Sniffing o escucha no autorizada: Interceptación de datos que circulan por la red.
- Spoofing: Suplantación de identidad en la red para acceder a información o sistemas restringidos.

Mecanismos de protección en redes

- Firewalls:
  Actúan como barreras entre redes internas confiables y redes externas no confiables (como Internet), bloqueando tráfico no autorizado.
- Cifrado (encriptación):
  Convierte los datos en un formato ilegible para que solo el destinatario correcto pueda entenderlos. Protocolos como HTTPS, SSL/TLS, y VPN cifran la información durante la transmisión.
- Antivirus y antimalware:
  Detectan y eliminan software malicioso que puede viajar a través de la red.
- Control de acceso a la red (NAC):
  Verifica la identidad y el estado del dispositivo antes de permitirle conectarse a la red.
- Autenticación multifactor (MFA):
  Requiere más de una forma de verificación (contraseña + código, huella digital, etc.) para acceder a la red o servicios.

- IDS y IPS (Sistemas de detección y prevención de intrusos): Detectan actividades sospechosas en la red y pueden bloquearlas automáticamente.

Buenas prácticas de seguridad en la red

- Cambiar contraseñas por defecto en routers y dispositivos.
- Usar contraseñas fuertes y únicas.
- Mantener los sistemas actualizados con los últimos parches de seguridad.
- Desconectar dispositivos que no estén en uso.
- Limitar el acceso a redes Wi-Fi con contraseñas seguras.
- Usar conexiones VPN en redes públicas.

Ejemplos comunes de aplicación

- Empresas: Implementan redes privadas virtuales (VPN), segmentación de redes y políticas de acceso para proteger información sensible.
- Hogares: Uso de firewalls en el router, contraseñas seguras y software antivirus para proteger los dispositivos personales.
- Escuelas y universidades: Controlan el tráfico de red mediante proxies y filtros de contenido para evitar accesos indebidos y proteger la red institucional.

Seguridad y protección para el usuario

La seguridad del usuario se refiere al conjunto de prácticas, herramientas y medidas que una persona debe adoptar para proteger su información personal y profesional cuando utiliza dispositivos y servicios digitales. Abarca desde la protección de contraseñas hasta el manejo seguro de archivos y el uso responsable de internet.

Principales riesgos para el usuario

- Robo de identidad: Cuando alguien obtiene y utiliza datos personales del usuario (como nombre, dirección o número de tarjeta).
- Phishing: Correos, mensajes o sitios falsos que intentan engañar al usuario para obtener información confidencial.
- Malware: Programas maliciosos que pueden dañar el dispositivo del usuario o robar su información.
- Redes Wi-Fi inseguras: Conectarse a redes públicas puede exponer los datos del usuario.
- Contraseñas débiles o repetidas: Facilitan que un atacante acceda a varias cuentas.

Medidas de protección para el usuario

- Crear contraseñas seguras:
  Usar combinaciones de letras mayúsculas, minúsculas, números y símbolos. No reutilizar contraseñas entre servicios.

- Usar autenticación de dos factores (2FA):
  Agrega una capa extra de seguridad al requerir un código adicional (como uno enviado al celular).
- No abrir enlaces sospechosos:
  Evitar hacer clic en correos electrónicos o mensajes no solicitados.
- Realizar copias de seguridad:
  Guardar información importante en la nube o dispositivos externos para evitar pérdidas por fallas o ataques.
- Actualizar el software:
  Tener el sistema operativo, antivirus y aplicaciones al día reduce vulnerabilidades.
- Cuidar lo que se comparte:
  Evitar publicar datos personales en redes sociales o sitios no confiables.
- Usar antivirus y antimalware confiables:
  Instalar programas que detecten amenazas en tiempo real.

Herramientas útiles para los usuarios

- Gestores de contraseñas: Como Bitwarden o LastPass para generar y almacenar contraseñas seguras.
- VPN: Protege la conexión, especialmente al usar redes públicas.
- Extensiones de navegador: Como bloqueadores de rastreadores o alertas de sitios peligrosos (ej. HTTPS Everywhere, Privacy Badger).
- Aplicaciones de verificación en dos pasos: Como Google Authenticator o Authy.

Ejemplo de escenarios comunes

- En casa: Un usuario protege su red Wi-Fi con contraseña segura, actualiza sus dispositivos, y no comparte su información bancaria por mensajes.
- En la escuela o trabajo: Un estudiante guarda sus archivos en la nube con respaldo, usa contraseñas fuertes para sus cuentas educativas y evita descargar software pirata.
- En redes sociales: Evita aceptar solicitudes de desconocidos y no comparte datos sensibles públicamente.

Conclusión

Con esta actividad logré entender de forma más clara la importancia de la seguridad en diferentes niveles: sistema operativo, red y usuario. Aunque ya habíamos visto estos temas en teoría, investigarlos por separado me permitió ver cómo cada uno cumple un rol específico para proteger la información.

Aprendí que el sistema operativo es clave para controlar accesos y proteger recursos, que la red necesita medidas como firewalls y cifrado, y que el usuario debe adoptar buenas prácticas para evitar errores comunes. En general, esta actividad me ayudó a

reforzar lo aprendido y a darle un enfoque más práctico a la seguridad en el entorno digital.

Fuentes

Ciberseguridad Tips. (s.f.). Qué es Seguridad y Protección en Sistemas Operativos: Guía completa 2023. Ciberseguridad Tips. https://ciberseguridadtips.com/proteccion-seguridad-sistemas-operativos/

IBM. (s.f.). Seguridad del sistema operativo. IBM Docs. https://www.ibm.com/docs/es/aix/7.2.0?topic=administration-operating-system-security

IBM. (s.f.). Seguridad de red. IBM. https://www.ibm.com/mx-es/topics/network-security

Check Point. (s.f.). ¿Qué es la seguridad de red? Check Point Cyber Hub. https://www.checkpoint.com/es/cyber-hub/network-security/what-is-network-security/

Safetica. (s.f.). Protección y seguridad de la información: una perspectiva de usuario. Safetica. https://www.safetica.com/es/blog/proteccion-y-seguridad-de-la-informacion-una-perspectiva-de-usuario

Universidad Veracruzana. (s.f.). El rol del usuario UV. InfoSegura UV. https://www.uv.mx/infosegura/concientizacion/campana/el-rol-del-usuario-uv/