I.E.S.T. PÚBLICO
FELIPE HUAMAN
POMA DE AYALA

UNIDAD DIDÁCTICA:

SISTEMAS OPERATIVOS



Tema:

Seguridad en Sistemas Operativos: Principios, Políticas y Control de Acceso

Docente: Ing. Elbir Diluvid Chuque Diaz

Programa de Estudios: Arquitectura de plataformas y servicios de Tecnologías de información

I.E.S.T. PÚBLICO
FELIPE HUAMAN
POMA DE AYALA

Acuerdos de convivencia

- Ingresar puntualmente y con los materiales necesarios.
- Mantener respeto hacia el docente y compañeros.
- Participar de manera ordenada, levantando la mano.
- Escuchar atentamente y evitar interrupciones.
- Usar el celular solo con fines académicos.
- Cumplir con las actividades y tiempos establecidos.
- Trabajar de forma colaborativa y responsable.

I.E.S.T. PÚBLICO
FELIPE HUAMAN
POMA DE AYALA

Sílabo

Seguridad en Sistemas Operativos: Principios, Políticas y Control de Acceso	Aplica principios de seguridad	**Sesión 7:** Principios de seguridad en sistemas operativos	2	1	**Sem. 4:** 04.05.2026 08.05.2026
	Implementa políticas básicas	**Sesión 8:** Políticas de seguridad y control de acceso	0	3	
Instalación de Sistemas Operativos: Requisitos Técnicos y Configuración de BIOS/UEFI	Prepara entorno de instalación	**Sesión 9:** Requisitos técnicos y configuración de BIOS/UEFI	2	1	**Sem. 5:** 11.05.2026 15.05.2026
	Ejecuta instalación de SO	**Sesión 10:** Proceso de instalación de sistemas operativos	0	3	

I.E.S.T. PÚBLICO
FELIPE HUAMAN
POMA DE AYALA

ACTIVIDADES DE INICIO



I.E.S.T. PÚBLICO
FELIPE HUAMAN
POMA DE AYALA

Sesión 5:
Seguridad en Sistemas Operativos: Principios, Políticas y Control de Acceso



Asignatura: Sistemas Operativos

Docente: Ing. Elbir Diluvid Chuque Diaz

I.E.S.T. PÚBLICO
FELIPE HUAMAN
POMA DE AYALA

Contenido

- Seguridad en Sistemas Operativos:
  - Principios
  - Políticas
  - Control de Acceso

Evidencia de aprendizaje

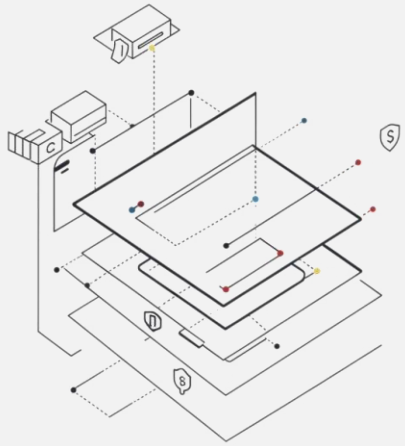
- Actividad formativa
- Instrumento de evaluación:

I.E.S.T. PÚBLICO
FELIPE HUAMAN
POMA DE AYALA

ACTIVIDADES DE DESARROLLO



¿Qué es la seguridad en un sistema operativo?



La seguridad en un sistema operativo es el **conjunto de mecanismos, normas y controles** que protegen:

- Los recursos del equipo
- La información almacenada
- Los procesos en ejecución
- El acceso de los usuarios

ⓘ Un SO seguro evita accesos no autorizados, pérdida de datos, modificaciones indebidas y uso incorrecto de los recursos del sistema.



Importancia de la seguridad en los SO

El sistema operativo administra los recursos más críticos del equipo. Una falla de seguridad tiene consecuencias graves.

🗂️ Recursos gestionados

Archivos, memoria, procesos, usuarios, dispositivos y conexiones de red.

⚠️ Riesgos de una falla

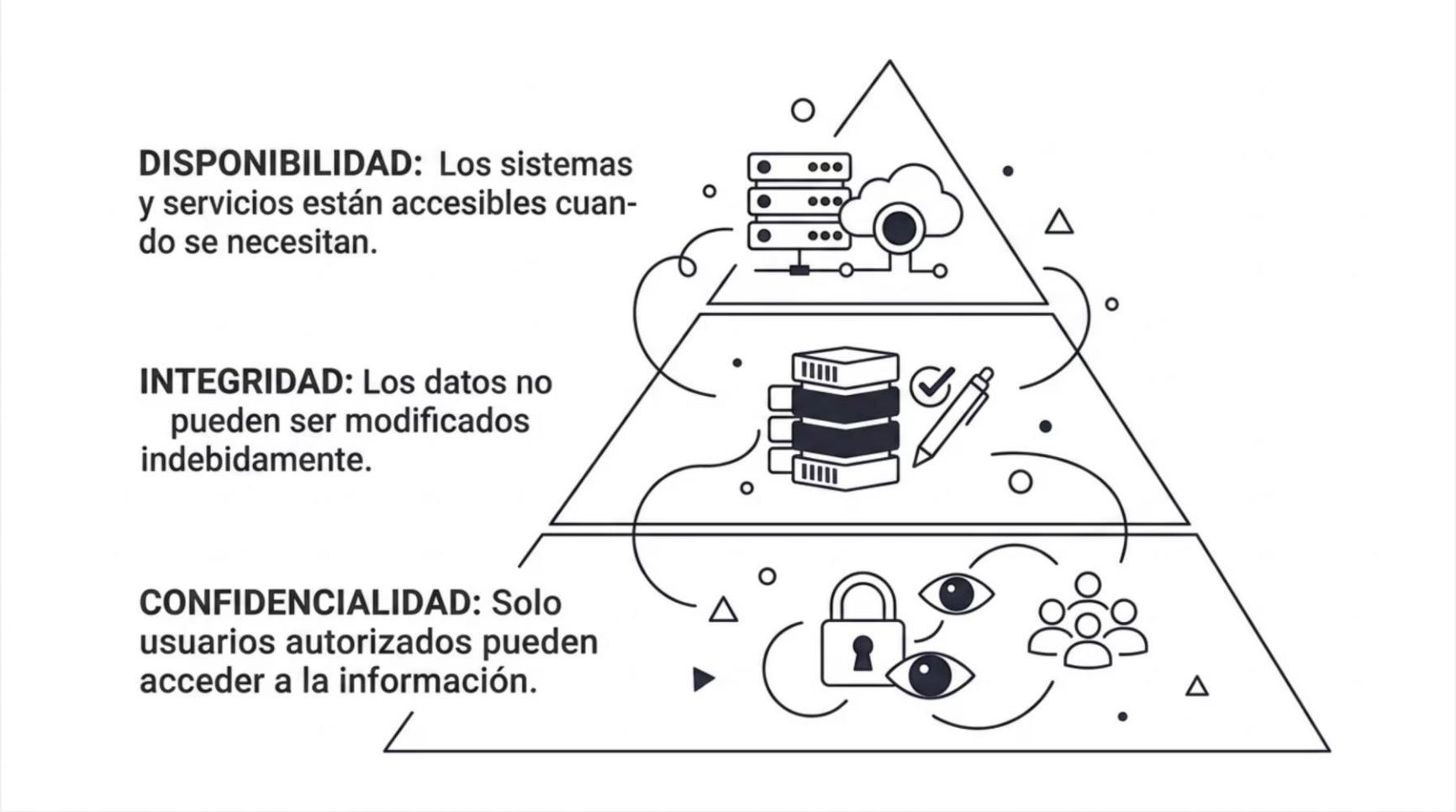
Pérdida de información, robo de datos, interrupción de servicios e instalación de malware.

🔐 Consecuencias reales

Acceso indebido a cuentas privadas, daños económicos y pérdida de confianza.

Principios de seguridad en SO

La seguridad informática se sustenta en tres pilares fundamentales conocidos como la **tríada CID**.



Principio de autenticación

La autenticación **verifica la identidad del usuario** antes de concederle acceso al sistema. Cuantos más factores se combinen, mayor es la seguridad.

****

Contraseña

El método más extendido.
Requiere clave secreta del usuario.

Huella digital

Autenticación biométrica basada en rasgos físicos únicos.

Reconocimiento facial

Identifica al usuario mediante rasgos del rostro.

Doble factor (2FA)

Combina contraseña con código enviado al móvil o tarjeta inteligente.

Principio de autorización



CONTROL DE ACCESO

Una vez autenticado, la autorización define **qué acciones puede realizar** un usuario dentro del sistema.

La autorización controla el acceso a carpetas, programas, dispositivos, configuraciones y recursos del sistema.

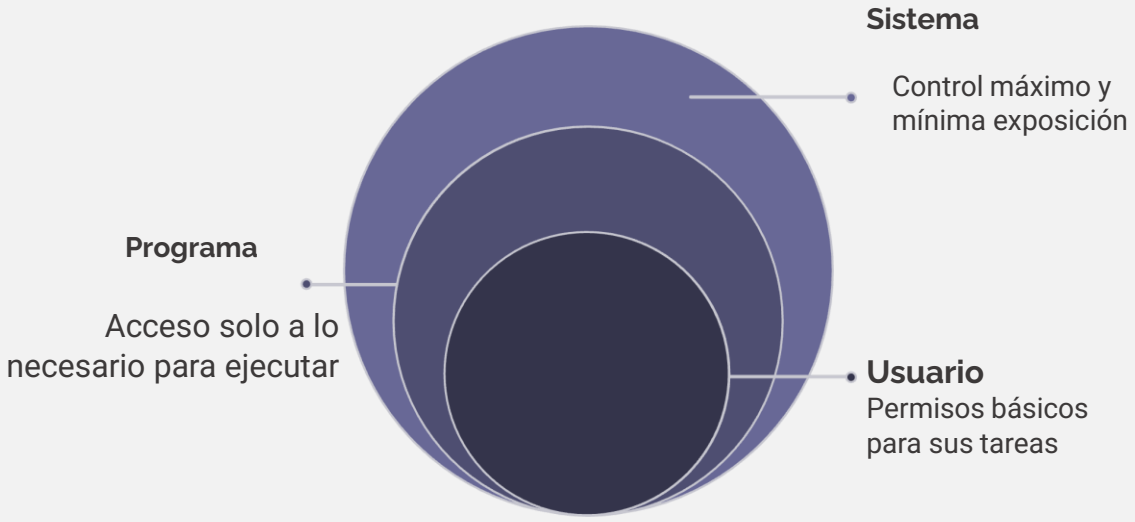
✅ **Permitido**

Leer archivos propios, ejecutar aplicaciones autorizadas.

❌ **Denegado**

Modificar, eliminar o acceder a archivos de otros usuarios o del sistema.

Principio de mínimo privilegio



Reducir privilegios limita el impacto de errores humanos, infecciones por malware y accesos indebidos.

¿Qué significa en la práctica?

Cada usuario, programa o proceso recibe **únicamente los permisos necesarios** para cumplir su función, y nada más.

⚠ Un estudiante no debería tener permisos de administrador en una computadora institucional. El exceso de privilegios aumenta la superficie de ataque.

Políticas de seguridad

Las políticas de seguridad son **reglas formales** que regulan cómo se usa y protege el sistema operativo y la información.

01

Comportamiento de usuarios

Definen cómo deben actuar los usuarios y qué permisos tienen asignados.

02

Gestión de contraseñas

Establecen requisitos de complejidad, caducidad y confidencialidad de las claves.

03

Instalación de software

Regulan qué programas se pueden instalar y quién tiene autorización para hacerlo.

04

Respuesta a incidentes

Indican cómo actuar ante una brecha de seguridad o incidente informático.



Políticas de contraseñas y roles de usuario

🔑 Buenas prácticas de contraseñas

- Contraseñas largas que combinen letras, números y símbolos
- Evitar nombres, fechas o palabras comunes
- Cambiarlas periódicamente y no compartirlas
- Activar la autenticación de doble factor siempre que sea posible

👥 Roles de usuario en el sistema

1

Administrador

Instala programas, crea usuarios y modifica configuraciones del sistema.

2

Usuario estándar

Usa aplicaciones y gestiona sus propios archivos sin acceso al sistema.

3

Invitado

Acceso limitado y temporal, sin posibilidad de cambios permanentes.

Control de acceso

¿Qué es?

El control de acceso es el mecanismo que **define quién puede ingresar a un recurso** y qué acciones puede realizar sobre él.

Su objetivo es evitar que usuarios no autorizados accedan, modifiquen o eliminen información importante del sistema.

- **Control de acceso discrecional:** el propietario del recurso decide quién puede acceder.
- **Control de acceso obligatorio:** el sistema aplica reglas estrictas de seguridad según niveles o categorías.
- **Control de acceso basado en roles:** los permisos se asignan según el rol del usuario dentro de la organización.
- El control basado en roles es muy usado en instituciones y empresas.



Amenazas comunes en sistemas operativos

Las principales amenazas son:

- Virus, troyanos y ransomware.
- Acceso no autorizado.
- Robo de contraseñas.
- Instalación de software malicioso.
- Errores de configuración.
- Uso de cuentas con demasiados privilegios.
- Eliminación o modificación accidental de archivos.
- Falta de actualizaciones de seguridad.

Estas amenazas pueden afectar el funcionamiento del sistema y comprometer la información.

Actividad formativa 01

Caso práctico:

En el laboratorio de cómputo del instituto, todos los estudiantes utilizan las mismas computadoras para realizar prácticas de programación, ofimática y navegación en internet. Sin embargo, en las últimas semanas se han presentado varios problemas: algunos estudiantes instalaron programas sin autorización, otros eliminaron archivos de sus compañeros y una computadora fue infectada con malware después de descargar un archivo desconocido. Además, se descubrió que varios usuarios compartían la misma contraseña para ingresar al sistema, y algunos estudiantes tenían permisos de administrador sin necesidad. Debido a esta situación, el área de soporte técnico decidió implementar nuevas políticas de seguridad, crear cuentas individuales para cada estudiante y asignar permisos según el rol de cada usuario.

Preguntas para resolver

1. Identificación del problema

¿Qué problemas de seguridad se presentan en el caso?
Menciona al menos tres problemas y explica brevemente por qué representan un riesgo para el sistema operativo.

2. Aplicación de principios de seguridad

¿Qué principios de seguridad se deberían aplicar para solucionar esta situación?
Explica cómo se aplicarían la confidencialidad, integridad, disponibilidad y mínimo privilegio en el laboratorio de cómputo.

3. Propuesta de solución

¿Qué políticas de seguridad y controles de acceso recomendarías implementar?
Propón al menos cuatro medidas concretas para proteger las computadoras, los archivos y las cuentas de usuario.

I.E.S.T. PÚBLICO
FELIPE HUAMAN
POMA DE AYALA

ACTIVIDADES DE CIERRE



Metacognición



- ¿Qué aprendí sobre la seguridad en los sistemas operativos y por qué es importante aplicarla?
- ¿Qué dificultades tuve al analizar el caso práctico y cómo las superé?
- ¿Cómo puedo aplicar lo aprendido para proteger mejor una computadora, mis archivos y mis cuentas de usuario?

Referencias

- Prieto Espinosa, A., Lloris Ruiz, A., & Torres Cantero, J. C. (2006). Introducción a la informática. McGraw-Hill.
- Beekman, G. (2005). Introducción a la informática. Pearson Educación.
- Joyanes Aguilar, L. (2020). Fundamentos de programación: Algoritmos, estructuras de datos y objetos. McGraw-Hill.

I.E.S.T. PÚBLICO
FELIPE HUAMAN
POMA DE AYALA

GRACIAS POR SU ATENCIÓN

