Sistema de Protección en Sistemas Operativos

Definición y función fundamental

Principios básicos de seguridad

Principio del privilegio mínimo

- **"Todo lo que no está expresamente permitido está prohibido"**
- Asignar mínimos privilegios por defecto
- Revisar periódicamente los permisos
- Registrar cambios en permisos de acceso

Protección de la información

- Salvaguardar **integridad** de los datos
- Garantizar **disponibilidad** de la información
- Implementar medidas de recuperación de datos
- Establecer procedimientos de copias de seguridad

Control de accesos fraudulentos

- Controlar intentos de acceso no autorizados
- Registrar fecha, hora y datos de intentos fallidos
- Almacenar información para descubrir autoría
- Establecer **mecanismos de alerta** ante múltiples intentos

Tipos de control de acceso

DAC
Control de Acceso Discrecional

El **propietario** del recurso decide quién puede acceder a él y con qué permisos

- Control total del propietario
- Listas de control de acceso (ACL)
- Flexible pero menos seguro

Ejemplos:

- Permisos Unix (rwx)
- Listas ACL en Windows NTFS

MAC
Control de Acceso Obligatorio

Políticas centralizadas que ningún usuario puede modificar

- Control estricto del sistema
- Etiquetas de seguridad
- Más seguro pero menos flexible

Ejemplos:

- SELinux en sistemas Linux
- System Integrity Protection

RBAC
Control de Acceso Basado en Roles

Asigna permisos a **roles** en lugar de a usuarios individuales

- Usuarios asignados a roles
- Administración simplificada
- Mejor auditoría y control

Ventajas:

- Escalabilidad en sistemas grandes
- Reducción de errores

Gestión de cuentas y permisos

Creación y administración de cuentas

Creación

Requiere **autorización** y documentación

Privilegios

Según **principio del mínimo privilegio**

Revisiones

Auditorías regulares de cuentas

Eliminación

Procedimientos para desactivación

Tipos de cuentas y privilegios

Administrador

Acceso **completo** al sistema

Estándar

Permisos **limitados** para actividades diarias

Invitado

Acceso muy **restringido**

Servicio

Para procesos del sistema

Buenas prácticas en gestión de permisos

- Evitar uso continuo de cuentas de **administrador**
- Implementar **autenticación de dos factores**
- Establecer políticas de contraseñas robustas
- Limitar usuarios con privilegios elevados

Mecanismos de protección avanzada

DEP
Prevención de Ejecución de Datos

Tecnología que **protege contra virus** y amenazas de seguridad

- Supervisa uso seguro de memoria
- Cierra programas con comportamiento sospechoso
- Notifica al usuario de actividades anómalas

Configuración:

- Activación para todos los programas
- Combinación con ASLR

Integridad
Protección de integridad del sistema

Mecanismos para **proteger componentes críticos** del sistema

- System Integrity Protection (SIP)
- Secure Boot para cadena de arranque
- Verificación de firmas digitales

Implementaciones:

- SIP en macOS
- UEFI Secure Boot

Aplicaciones
Control de aplicaciones

Mecanismos para **controlar ejecución** de software

- AppLocker en Windows
- Gatekeeper en macOS
- Sandboxing para aislamiento

Técnicas:

- Listas blancas/negras
- Verificación de firmas

Gestión de amenazas y vulnerabilidades

Tipos de amenazas

Malware

Virus, gusanos, troyanos, ransomware

Denegación de servicio

Consumo de recursos del sistema

Elevación de privilegios

Acceso no autorizado al sistema

Estrategias de mitigación

- Firewalls integrados para tráfico de red
- Actualizaciones de seguridad regulares
- Protección en tiempo real contra amenazas
- Mecanismos de aislamiento de procesos
- Auditoría y registro de actividades

Gestión de vulnerabilidades

- Monitoreo constante de vulnerabilidades
- Evaluación de riesgos para priorizar parches
- Pruebas de penetración para identificar debilidades
- Gestión de parches y actualizaciones
- Planes de respuesta a incidentes

Tendencias actuales en seguridad

Seguridad en hardware

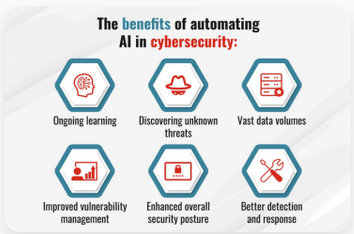
- **TPM 2.0**: Módulos de seguridad integrados
- Encriptación basada en hardware
- Protecciones contra Spectre y Meltdown

Seguridad en la nube

- **Identidad como servicio**: Gestión centralizada
- Protección de datos en reposo y en tránsito
- Seguridad basada en políticas en entornos híbridos

Inteligencia Artificial

- **Detección de anomalías** en comportamientos
- Respuesta automatizada a incidentes
- Predicción de amenazas basada en patrones



Seguridad IoT y Edge

- Protección de dispositivos con **recursos limitados**
- Gestión segura de actualizaciones remotas
- Autenticación robusta en entornos edge