Windows 11 – Políticas de Seguridad

Windows 11 incluye mejoras de seguridad significativas respecto a versiones anteriores. Microsoft ha adoptado una política de "seguridad por diseño" y exige ciertos requisitos de hardware para habilitar estas características.

Principales Políticas y Características de Seguridad:

1. **Requisitos de hardware seguro:**
    - **TPM 2.0 (Trusted Platform Module):** Obligatorio para el cifrado de datos y autenticación segura.
    - **Arranque seguro (Secure Boot):** Evita la carga de software malicioso durante el inicio.
2. **Protección del sistema operativo:**
    - **Virtualization-Based Security (VBS):** Aísla procesos críticos del sistema operativo.
    - **Hypervisor-Enforced Code Integrity (HVCI):** Protege contra ataques a nivel de kernel.
3. **Microsoft Defender Antivirus y SmartScreen:**
    - Protección integrada contra malware, ransomware y sitios web maliciosos.
    - Smart App Control bloquea aplicaciones no confiables (disponible en versiones recientes).
4. **Actualizaciones automáticas:**
    - Las actualizaciones de seguridad se distribuyen mensualmente (Patch Tuesday).
    - Las políticas empresariales pueden forzar tiempos específicos de instalación.
5. **Identidad y acceso:**
    - **Windows Hello:** Autenticación biométrica o PIN seguro.
    - **BitLocker:** Cifrado de disco completo.

- **Credential Guard:** Protege credenciales almacenadas en la memoria.

6. **Seguridad para empresas (con Microsoft Defender for Endpoint):**
    - Supervisión avanzada de amenazas (ATP).
    - Gestión de dispositivos y cumplimiento normativo con Microsoft Intune y Azure AD.

Ubuntu 24.04 LTS – Políticas de Seguridad

Ubuntu 24.04 LTS ("Noble Numbat") mantiene el enfoque tradicional de Canonical hacia la seguridad: actualizaciones constantes, configuraciones predeterminadas seguras y soporte a largo plazo (5 años).

Principales Políticas y Características de Seguridad:

1. **Modelo de seguridad proactivo:**
    - **AppArmor**: Sistema Mandatory Access Control (MAC) por defecto para restringir el acceso a recursos por parte de aplicaciones.
    - **Seccomp (Secure Computing Mode):** Filtra llamadas al sistema que pueden ser peligrosas.
    - **Kernel Lockdown Mode:** Refuerza el modo de integridad del kernel.
2. **Cifrado y autenticación:**
    - **Full disk encryption** con LUKS en instalaciones estándar.
    - **Autenticación basada en PAM** y soporte para FIDO2/U2F para login.
3. **Actualizaciones de seguridad:**
    - **Livepatch** permite aplicar parches de seguridad al kernel sin reiniciar.
    - **Soporte extendido (LTS):** Hasta abril de 2030 con Ubuntu Pro.
4. **Privacidad y aislamiento de procesos:**
    - **Snap packages:** Aislados con sandboxing.

    - **Wayland (por defecto):** Mayor aislamiento gráfico que X11.

5. **Herramientas para administración segura:**
    - **ufw (Uncomplicated Firewall):** Firewall simple por defecto.
    - **fail2ban:** Protección contra ataques de fuerza bruta.
    - **Canonical Landscape o Ubuntu Pro:** Gestión centralizada de políticas de seguridad para múltiples máquinas.
6. **Auditoría y cumplimiento:**
    - Compatible con herramientas de cumplimiento como CIS Benchmark, OpenSCAP y más.
    - Soporte para SELinux y otros frameworks opcional.

Elementos para implementar

1. Acceso y Autenticación

- MFA obligatorio (2FA).
- Integración con Active Directory/LDAP.
- Windows: usar Windows Hello.
- Ubuntu: usar PAM + FIDO2.

2. Cifrado

- Cifrado de disco completo obligatorio:
    - Windows: BitLocker.
    - Ubuntu: LUKS.

3. Actualizaciones

- Parches críticos semanales.

- Windows: WSUS o Intune.
- Ubuntu: Livepatch + Landscape/Ansible.

4. Antivirus y Firewall

- Antivirus en todos los equipos.
    - Windows: Microsoft Defender.
    - Ubuntu: ClamAV (u otro).
- Firewall activo:
    - Windows Firewall / UFW.

5. Hardening

- Solo software aprobado.
- Windows: GPO + Smart App Control.
- Ubuntu: AppArmor activo.

6. Monitoreo

- Centralización de logs (SIEM).
- Auditorías activas en ambos sistemas.

7. Backups

- Copias automáticas diarias, cifradas y externas.
- Pruebas regulares de recuperación.