**ÍNDICE DEL APARTADO DE SEGURIDAD (Víctor)**

# 1. POLÍTICAS GENERALES DE SEGURIDAD

## 1.1. Justificación de la seguridad como parte integral del proyecto

La seguridad informática es un componente importante e inseparable en el diseño, implementación y operación de cualquier infraestructura tecnológica moderna. En relación con este proyecto, que se basa en Windows y Linux, la introducción y comparación de pequeñas empresas, la seguridad cibernética después de la implementación no debe considerarse una fase, sino como una necesidad estructural ya que el sistema está establecido.

Esta integración temprana es particularmente crítica para el entorno de las PYME, donde los recursos son limitados y la exposición al riesgo puede poner en peligro la continuidad del negocio. La introducción de medidas de seguridad desde el principio permite una reducción significativa en el riesgo operativo al prevenir los ataques, el acceso no autorizado o la pérdida de información, situaciones que podrían tener una reputación financiera y de reputación significativa. También facilita el cumplimiento legislativo, ya que garantiza un marco legal, como GDPR, que proporciona trazabilidad, acceso suficiente y protección de datos personales.

Además, en realidad brinda la oportunidad de proteger los activos más críticos de la empresa, como bases de datos de clientes, documentos internos o de identificación a través de herramientas de cifrado, políticas de usuario y planes de repuesto apropiados. La infraestructura establecida con criterios de seguridad también promueve eventos de resistencia, incluso desde el comienzo del diseño, como robustos, segmentación de red, control del tráfico y restauración de errores o ataques.

Desde un punto de vista práctico, se utiliza en la evaluación de riesgos inicial, en la definición de requisitos de seguridad no funcionales, incluidas las tareas asociadas y la suposición de una responsabilidad común entre todos los miembros del equipo. Esta visión transversal proporciona protección continua, mejora la calidad general del sistema y promueve el éxito del proyecto no solo desde un punto de vista técnico, sino también desde las actividades y las perspectivas estratégicas de la organización.

## 1.2. Comparativa del enfoque de seguridad en Windows y Linux

Windows 11 ofrece un método de seguridad mejorado desde el principio. TPM 2.0 requiere un inicio obligatorio y seguro (troncal seguro) y una compañía UEFI que garantiza un entorno más protegido contra el software malicioso que opera antes de que se cargue el sistema.

En el caso de Linux, la seguridad se basa en un modelo de control más granular. Aunque no incluye VBS o HVCI, distribuciones como Ubuntu o Fedora integran sistemas de control de acceso como AppArmor y SELinux, que restringen el comportamiento de procesos sensibles. Además, Linux es compatible con TPM y Secure Boot, y permite una gestión manual de servicios, permisos y actualizaciones, dando al administrador mayor control del entorno.

## 1.3. Establecimiento de políticas de seguridad según perfil de usuario

**Introducción**

Las políticas de seguridad sirven para limitar el riesgo operativo y aplicar el principio de mínimo privilegio. Nos hemos basado en las políticas como base de las plantillas y directrices del INCIBE (Instituto Nacional de Ciberseguridad)

**Administrador de sistemas**

* Uso de credenciales personales con autenticación segura; recomendación de doble factor (2FA) en accesos críticos.
* Cuentas separadas para tareas administrativas y uso diario.
* Registro de logs de actividad administrativa y revisión periódica.
* Acceso remoto restringido mediante VPN o redes autorizadas.
* Documentación obligatoria de cambios críticos en la infraestructura.
* Prohibición de utilizar dispositivos personales para acceder al sistema.

**Usuario estándar**

* Acceso limitado exclusivamente a los recursos necesarios para su función.
* Prohibición de instalación o modificación de software no autorizado.
* Uso obligatorio de contraseñas seguras (mínimo 10 caracteres, alfanuméricas), con renovación cada 90 días.
* Bloqueo automático de sesión tras un máximo de 10 minutos de inactividad.
* Antivirus activo y actualizado permanentemente.
* Uso restringido de dispositivos externos (USB, discos portátiles) no autorizados.
* Prohibición de almacenar datos en el escritorio local o dispositivos externos.

**Técnico o desarrollador**

* Acceso autorizado a terminales, entornos de desarrollo, compiladores, contenedores y máquinas virtuales.
* Prohibición de privilegios administrativos en sistemas de producción sin autorización expresa.
* Uso de control de versiones obligatorio para scripts y automatizaciones.
* Revisión y documentación de toda actividad técnica realizada.
* Uso exclusivo de herramientas validadas por la organización.

**Usuario temporal o invitado**

* Cuentas temporales con fecha de caducidad predefinida.
* Acceso restringido a funciones básicas y no persistente (sin almacenamiento local).
* Prohibición de acceso a carpetas compartidas internas o documentación sensible.
* Eliminación automática de la cuenta una vez concluida la actividad prevista.

**Políticas comunes a todos los usuarios**

* Uso obligatorio de contraseñas robustas y personales.
* Prohibido compartir credenciales de acceso.
* Eliminación de cuentas inactivas tras 30 días sin uso.
* Revisión periódica de los permisos asignados en función del rol.
* Uso exclusivo de software autorizado y actualizado.
* Almacenamiento de archivos únicamente en ubicaciones seguras designadas por el administrador.
* Bloqueo manual de sesión al ausentarse del puesto.
* Custodia física adecuada de dispositivos móviles o portátiles.
* Participación en formación básica en ciberseguridad (navegación, correo, identificación de amenazas).

**Medidas adicionales complementarias**

* Solo se permite el uso de dispositivos USB previamente autorizados por el administrador.
* Cualquier unidad externa deberá ser escaneada antes de su utilización.
* El uso de impresoras compartidas estará sujeto a control de acceso y podrá ser auditado si la infraestructura lo permite.
* Se realizará una auditoría mensual del inventario de cuentas. Las cuentas de usuarios dados de baja serán eliminadas de inmediato.
* En caso de detección de accesos no autorizados o comportamiento anómalo, se notificará de inmediato al administrador, quien registrará el incidente conforme al protocolo interno.

**2. ENDURECIMIENTO (HARDENING) DEL SISTEMA**

El hardening del sistema cosiste en aplicar una serie de medidas técnicas y organizativas que reducen la superficie de exposición a posibles ataques, eliminando o restringiendo funcionalidades no necesarias y aplicando configuraciones seguras minimizando así vulnerabilidades explotables, para poder aumentar el control de los sistemas y proteger la información sensible

2.1. Desactivación de servicios innecesarios

Una de las primeras acciones en el endurecimiento de un sistema es la identificación y desactivación de servicios y procesos que no son necesarios para el funcionamiento previsto del equipo. Esto reduce el consumo de recursos y elimina posibles vectores de ataque, especialmente si los servicios están expuestos a la red.

  2.1.1. Windows

En sistemas Windows, se recomienda revisar el listado de servicios desde la consola de servicios (services.msc) o mediante herramientas de administración de políticas de grupo. Algunos servicios innecesarios en entornos corporativos pueden incluir:

* **Fax**: en desuso en muchas oficinas.
* **Bluetooth**: si el equipo no requiere conectividad inalámbrica de corto alcance.
* **Windows Remote Registry**: innecesario salvo en entornos de administración centralizada.
* **XPS Services**: funcionalidad de impresión que puede ser sustituida por PDF.
* **Servidores multimedia o servicios de juegos**.

La desactivación debe realizarse de forma controlada, comprobando que no afecta a la funcionalidad general ni a procesos críticos. Se recomienda crear una política de grupo o script de desactivación estándar.

  2.1.2. Linux

En entornos Linux, la gestión de servicios se realiza mediante systemctl, service o herramientas específicas de cada distribución. Algunos servicios que pueden desactivarse si no se utilizan son:

* **Avahi-daemon** (descubrimiento de red).
* **rpcbind** (llamadas a procedimientos remotos).
* **telnet**, **ftp**: protocolos obsoletos y no cifrados.

Se puede utilizar el comando systemctl list-unit-files --type=service para listar todos los servicios y su estado, y desactivar aquellos innecesarios con systemctl disable nombre-del-servicio.

2.2. Configuración segura del arranque y la BIOS/UEFI

La protección del proceso de arranque es crítica para evitar la manipulación del sistema antes de que el control pase al sistema operativo. Las siguientes recomendaciones son aplicables a sistemas modernos:

* **Activar Secure Boot** desde la BIOS/UEFI para impedir el arranque de sistemas no firmados.
* **Establecer una contraseña de acceso a la BIOS/UEFI** para evitar modificaciones no autorizadas.
* **Desactivar el arranque desde dispositivos externos** (USB, DVD) si no son necesarios, reduciendo el riesgo de bootkits o cargas no autorizadas.
* **Activar el arranque desde disco interno en primer lugar** y bloquear cambios sin autenticación.
* En entornos Windows 11, **la presencia de TPM 2.0 y UEFI** fortalece el entorno de arranque frente a amenazas de bajo nivel.

Estas medidas refuerzan la integridad del sistema desde el encendido hasta la carga completa del sistema operativo.

2.3. Aplicación de recomendaciones de buenas prácticas (CIS Benchmarks, Lynis)

Para complementar las medidas anteriores, se recomienda aplicar guías de buenas prácticas y realizar auditorías automatizadas de seguridad. Dos herramientas destacadas en este ámbito son:

* **CIS Benchmarks (Center for Internet Security)**: proporciona guías detalladas y actualizadas con configuraciones recomendadas para múltiples sistemas (Windows, Linux, dispositivos de red, etc.). Estas guías permiten asegurar parámetros como:
  + Políticas de contraseñas.
  + Configuración de auditoría de eventos.
  + Restricciones en servicios y puertos.
  + Permisos de archivos y registros.
  + Seguridad en el navegador y actualizaciones automáticas.
* **Lynis (Linux Audit Tool)**: herramienta de auditoría de seguridad automatizada para sistemas Linux y Unix. Permite identificar configuraciones inseguras, servicios activos innecesarios, permisos incorrectos, entre otros. Proporciona un informe con puntuación de seguridad y recomendaciones prácticas para su mejora.

Ambas herramientas permiten estandarizar y verificar el cumplimiento de políticas de seguridad en los sistemas, facilitando la gestión continua del hardening.

**4. FIREWALL Y CONTROL DE TRÁFICO**

4.1. Configuración del cortafuegos en Windows (Defender Firewall)

**Windows Defender Firewall** es la solución integrada en los sistemas Windows para la gestión del tráfico de red. Permite aplicar reglas específicas por tipo de red (pública, privada o de dominio) y controlar el acceso por aplicación o puerto.

**Pasos recomendados:**

* Activar el firewall en los tres perfiles (privado, público y de dominio).
* Bloquear todas las conexiones entrantes por defecto y permitir solo las necesarias.
* Crear reglas explícitas para permitir servicios esenciales (ej. Escritorio remoto, SMB compartido con seguridad, etc.).
* Restringir las aplicaciones que pueden comunicarse con el exterior.
* Revisar las reglas preconfiguradas y desactivar aquellas que no sean necesarias

4.2. Configuración del cortafuegos en Linux (UFW o firewalld)

En sistemas Linux, el cortafuegos por excelencia es **iptables**, pero por simplicidad de uso se emplean interfaces como **UFW** (Ubuntu/Debian) o **firewalld** (Fedora/CentOS/RHEL).

**UFW (Uncomplicated Firewall)**

* Se activa con: sudo ufw enable
* Reglas básicas:

sudo ufw default deny incoming  
sudo ufw default allow outgoing

sudo ufw allow ssh

sudo ufw allow 80/tcp

Ver estado y reglas:

sudo ufw status verbose

**firewalld**

* Utiliza zonas de red y es más dinámico.
* Activación: sudo systemctl enable --now firewalld
* Configurar zonas:

sudo firewall-cmd --zone=public --add-port=22/tcp --permanent

sudo firewall-cmd --reload

4.3. Aplicación de reglas según zonas de red y roles

Es recomendable definir reglas de firewall **según el contexto de red** y **los roles de los dispositivos**:

* **Zona interna (LAN):** permitir puertos específicos como SMB, RDP o SSH si son necesarios, con control de IP origen.
* **Zona pública (Internet):** bloquear todo por defecto y permitir solo servicios estrictamente necesarios (ej. HTTP/HTTPS en servidores web).
* **Zona de gestión:** red interna protegida donde solo accede el equipo de administración (IP restringidas).

**Por roles:**

* **Servidores:** abrir solo los puertos del servicio que ofrecen (ej. 80/443 para web, 22 para SSH).
* **Clientes/Usuarios:** bloquear puertos innecesarios de entrada y salida (ej. puertos de juegos, P2P, etc.).
* **Equipos administrativos:** permitir acceso solo a servicios de gestión seguros, y registrar el tráfico de administración.

Estas reglas deben estar documentadas y ser coherentes con la arquitectura de red definida.

**5. ANTIVIRUS Y PROTECCIÓN ANTIMALWARE**

5.1. Soluciones integradas en Windows (Windows Defender)

**Microsoft Defender Antivirus** (anteriormente Windows Defender) es la solución nativa de Windows 10 y 11, incluida sin coste adicional. Su integración con el sistema operativo permite una protección en tiempo real eficaz y sin interferencias significativas en el rendimiento.

**Características destacadas:**

* Protección en tiempo real y análisis bajo demanda.
* Monitorización de comportamiento con protección contra ransomware (mediante "Acceso controlado a carpetas").
* Integración con el **Centro de Seguridad de Windows**.
* Actualizaciones automáticas a través de Windows Update.
* Compatible con políticas de grupo y administración remota mediante PowerShell o Intune.

Para entornos corporativos pequeños, Defender es una solución más que suficiente si se complementa con buenas prácticas y políticas de restricción de ejecución

5.2. Implementación de antivirus en Linux (ClamAV u otros)

Aunque los sistemas Linux son menos propensos a malware convencional, pueden actuar como **puentes de infección** en redes mixtas o estar expuestos a amenazas específicas (scripts maliciosos, exploits, troyanos).

**ClamAV** es el antivirus de código abierto más común para entornos Linux:

* Permite escaneo bajo demanda y programación de análisis periódicos.
* Se actualiza regularmente mediante freshclam.
* Compatible con la exploración de directorios compartidos, servidores de correo, y servidores web.

5.3. Análisis periódicos y gestión de amenazas

5.4. Buenas prácticas para la prevención de malware

**6. GESTIÓN DE USUARIOS Y PERMISOS**

6.1. Aplicación del principio de mínimo privilegio  
6.2. Configuración segura de sudoers (Linux)  
6.3. Políticas locales de control de cuentas (UAC, GPOs en Windows)  
6.4. Control de accesos remotos (SSH, RDP)  
6.5. Auditoría de permisos y accesos

**7. REGISTROS Y MONITORIZACIÓN**

7.1. Registros del sistema en Linux (/var/log, journalctl)  
7.2. Visor de eventos de Windows (Security, System, Application)  
7.3. Configuración de rotación y conservación de logs  
7.4. Procedimientos básicos de análisis de logs y recolección de evidencias

**8. CIFRADO Y PROTECCIÓN DE DATOS**

8.1. Cifrado de unidades (BitLocker en Windows, LUKS en Linux)  
8.2. Cifrado de archivos sensibles y backups  
8.3. Gestión de claves y contraseñas seguras  
8.4. Verificación de integridad de datos críticos

**9. BACKUPS Y RECUPERACIÓN**

9.1. Política de copias de seguridad (locales y externas)  
9.2. Automatización de copias mediante cron y tareas programadas  
9.3. Encriptación y control de acceso a copias de seguridad  
9.4. Pruebas de restauración y documentación del procedimiento

**10. SEGURIDAD EN REDES**

10.1. Configuración segura de interfaces de red y DNS  
10.2. Limitación de servicios expuestos  
10.3. Control de accesos remotos con autenticación fuerte  
10.4. Prevención de escaneos y ataques comunes (fail2ban, configuración de firewall)

**11. AUDITORÍA BÁSICA DE SEGURIDAD**

11.1. Comprobaciones de puertos y servicios activos  
11.2. Revisión de configuraciones críticas  
11.3. Análisis de eventos sospechosos en registros  
11.4. Informe de riesgos detectados y medidas aplicadas  
11.5. Recomendación profesional: implantación futura de sistemas IDS

**12. INTEGRACIÓN DE LA SEGURIDAD EN LA METODOLOGÍA ÁGIL**

12.1. Inclusión de tareas de seguridad en el backlog de producto  
12.2. Seguridad como parte del “Definition of Done” en cada Sprint  
12.3. Revisiones de seguridad planificadas en reuniones de Sprint Review  
12.4. Responsabilidades de los roles Scrum respecto a la ciberseguridad