**ÍNDICE FINAL DEL APARTADO DE SEGURIDAD**

# 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

### 1.3.1 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)

### 1.3.2 Políticas de seguridad por perfil de usuario

* Administrador de sistemas
  + Uso exclusivo de cuentas administrativas para tareas críticas
  + Revisión y auditoría periódica de los logs de administración
* Usuario estándar (empleados)
* Técnico o desarrollador
* Usuario temporal o invitado

1.3.4 Políticas comunes a todos los usuarios

1.3.5 Políticas complementarias aplicables

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

2.1. Desactivación de servicios innecesarios  
  2.1.1. Windows  
  2.1.2. Linux  
2.2. Configuración segura del arranque y la BIOS/UEFI  
2.3. Aplicación de recomendaciones de buenas prácticas (CIS Benchmarks, Lynis)

**3. GESTIÓN DE ACTUALIZACIONES Y PARCHES**

3.1. Configuración de actualizaciones automáticas  
3.2. Control y registro de actualizaciones críticas  
3.3. Automatización de tareas de actualización (scripts, tareas programadas)

**4. FIREWALL Y CONTROL DE TRÁFICO**

4.1. Configuración del cortafuegos en Windows (Defender Firewall)  
4.2. Configuración del cortafuegos en Linux (UFW o firewalld)  
4.3. Aplicación de reglas según zonas de red y roles  
4.4. Verificación y exportación de reglas de seguridad

**5. ANTIVIRUS Y PROTECCIÓN ANTIMALWARE**

5.1. Soluciones integradas en Windows (Windows Defender)  
5.2. Implementación de antivirus en Linux (ClamAV u otros)  
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