Tabla de contenido

1. Propósito 1

2. Alcance 2

2.1. Dispositivos de Comunicación y Red (Networking) 2
2.2. Servidores y Almacenamiento 3
2.3. Periféricos y Dispositivos de Oficina 3
2.4. Infraestructura de Seguridad y Videovigilancia 3
2.5. Ciclo de Vida del Activo 3

3. Políticas de Configuración Segura (Hardening) 4

3.1. Establecimiento de Líneas Base (Baselines) 4
3.2. Gestión de Credenciales y Acceso 4
3.3. Minimización de Servicios y Puertos (Principio de Necesidad) 4
3.4. Protección de Interfaces y Periféricos 4
3.5. Actualizaciones y Parches de Seguridad 5
3.6. Gestión de Banners y Mensajes de Sistema 5

4. Procedimientos 5

4.1. Fase de Preparación y Selección de Baseline 5
4.2. Ejecución del Endurecimiento (Hardening) 5
4.3. Llenado del Registro de Hardening 6
4.4. Pruebas de Verificación (QA de Seguridad) 6
4.5. Liberación a Producción e Inventario 6
4.6. Auditoría de Mantenimiento (Re-Hardening) 7

5. Definiciones 7

6. Formatos 7

7. Relación Normativa (ISO 27001:2022) 8

1. Propósito

El presente documento tiene como objetivo establecer los lineamientos técnicos y administrativos para el endurecimiento (**Hardening**) de todos los activos de infraestructura tecnológica del H. Ayuntamiento de Morelia. Se busca reducir al mínimo la superficie de ataque mediante la eliminación de servicios, protocolos y funciones innecesarias,

asegurando que cada dispositivo opere bajo un estado de seguridad óptimo y estandarizado.

A través de esta política, se persiguen los siguientes objetivos estratégicos:

- **Reducción de la Superficie de Exposición:** Garantizar que solo los servicios y puertos estrictamente necesarios para la operación institucional estén activos, mitigando riesgos de explotación de vulnerabilidades conocidas.
- **Estandarización de la Infraestructura:** Establecer una "Línea Base de Seguridad" (Baseline) uniforme para cada categoría de activo (Servidores, Switches, Routers, Cámaras, etc.), evitando configuraciones heterogéneas que dificulten la gestión de seguridad.
- **Protección contra Accesos No Autorizados:** Asegurar que todos los activos cuenten con mecanismos robustos de autenticación, eliminando credenciales por defecto y configuraciones de fábrica inseguras.
- **Aseguramiento del Cumplimiento Normativo:** Alinearse con los controles de la **ISO 27001:2022** referentes a la gestión de la configuración, proporcionando evidencia auditable a través del **Registro de Hardening**.
- **Prevención de Movimientos Laterales:** Blindar los equipos de comunicación y periféricos (como centros de impresión y módems) para evitar que sean utilizados como puntos de entrada o pivoteo en caso de una intrusión en la red.
- **Trazabilidad de la Configuración:** Mantener un historial detallado de los parámetros de seguridad aplicados a cada activo, facilitando las auditorías técnicas y la reconstrucción de la postura de seguridad ante cambios o incidentes.

2. Alcance

Esta política es de **cumplimiento obligatorio** para todo el personal de la Dirección de TI, administradores de red, responsables de infraestructura y proveedores externos que realicen la instalación o mantenimiento de equipos. El alcance comprende la aplicación del proceso de endurecimiento en los siguientes activos:

2.1. Dispositivos de Comunicación y Red (Networking)

- **Switches y Routers:** Configuración segura de puertos, desactivación de protocolos no cifrados (Telnet, HTTP) y gestión de VLANs.
- **Módems y Access Points (Wi-Fi):** Cambio de credenciales de administración, ocultamiento de SSIDs no públicos y uso de cifrado WPA3 o WPA2-Enterprise.

- **Firewalls:** Aplicación de reglas de denegación por defecto y limpieza de políticas obsoletas.

2.2. Servidores y Almacenamiento

- **Sistemas Operativos:** Hardening de Windows Server y distribuciones Linux (desactivación de servicios innecesarios, políticas de contraseñas locales).
- **Bases de Datos:** Restricción de conexiones remotas, cambio de puertos por defecto y eliminación de usuarios de ejemplo.

2.3. Periféricos y Dispositivos de Oficina

- **Centros de Impresión (Multifuncionales):** Desactivación de servicios de red innecesarios (FTP, SNMP v1/v2), borrado automático de memoria y protección de la interfaz web de administración.
- **Equipos de Cómputo Final:** Laptops y PCs de escritorio (bloqueo de puertos USB, eliminación de software bloatware).

2.4. Infraestructura de Seguridad y Videovigilancia

- **Cámaras de Seguridad (IP):** Cambio de contraseñas de fábrica, actualización de firmware y aislamiento en redes exclusivas para CCTV.
- **Grabadores (NVR/DVR):** Restricción de acceso desde internet y cifrado de las transmisiones de video.

2.5. Ciclo de Vida del Activo

El proceso de endurecimiento rige en los siguientes momentos:

- **Instalación Inicial:** Ningún equipo se conecta a la red de producción sin antes haber completado su **Registro de Hardening**.
- **Actualizaciones Mayores:** Tras un cambio de versión de firmware o sistema operativo.
- **Auditorías Periódicas:** Revisión semestral para asegurar que la configuración segura no se haya degradado.

3. Políticas de Configuración Segura (Hardening)

3.1. Establecimiento de Líneas Base (Baselines)

- **Estandarización:** Cada categoría de activo (Networking, Servidores, Impresión, CCTV) debe contar con una "Configuración Base" documentada. Se preferirá el uso de estándares internacionales como los **CIS Benchmarks**(Center for Internet Security) adaptados a la realidad operativa del Ayuntamiento.
- **Documentación Previa:** No se autorizará la puesta en marcha de ningún activo que no cuente con su respectivo **Registro de Hardening** debidamente requisitado.

3.2. Gestión de Credenciales y Acceso

- **Eliminación de Valores de Fábrica:** Es estrictamente obligatorio el cambio de todas las contraseñas predeterminadas (ej. admin/admin, root/1234) antes de conectar el equipo a la red.
- **Cuentas Nominales:** Se deben desactivar o renombrar las cuentas de administrador genéricas. El acceso a la configuración de los equipos (Switches, Routers, Módems) debe ser nominal y rastreable.
- **Autenticación Robusta:** Siempre que el hardware lo permita, se activará la autenticación multifactor (MFA) o el uso de certificados para el acceso administrativo.

3.3. Minimización de Servicios y Puertos (Principio de Necesidad)

- **Regla de Denegación por Defecto:** Todo servicio, protocolo o puerto que no sea estrictamente necesario para la función del equipo debe ser desactivado o bloqueado (ej. desactivar servicios de impresión en un servidor de archivos o protocolos de descubrimiento en cámaras IP).
- **Protocolos Seguros:** Se prohíbe el uso de protocolos de administración en texto plano (como Telnet, HTTP o FTP). Es obligatorio el uso de versiones cifradas (SSH, HTTPS, SFTP, SNMPv3).

3.4. Protección de Interfaces y Periféricos

- **Cierre de Puertos Físicos:** Los puertos de red (ethernet) en áreas comunes que no estén en uso deben ser desactivados lógicamente en el Switch.
- **Interfaces de Gestión:** Las interfaces web de administración (de módems, impresoras y cámaras) solo deben ser accesibles desde la VLAN de gestión administrativa, nunca desde la red de usuarios o internet abierto.

- **Restricción de Hardware:** En equipos finales, se deben bloquear los puertos USB para dispositivos de almacenamiento masivo, a menos que exista una justificación técnica aprobada.

3.5. Actualizaciones y Parches de Seguridad

- **Firmware y Parcheo:** El proceso de Hardening incluye la actualización del software o firmware a la última versión estable de seguridad antes de su despliegue.
- **Monitoreo de Vulnerabilidades:** Se deben realizar escaneos periódicos para verificar que la configuración segura no se haya visto comprometida por nuevas vulnerabilidades descubiertas.

3.6. Gestión de Banners y Mensajes de Sistema

- **Ocultamiento de Información:** Los banners de bienvenida de los equipos no deben mostrar información técnica (versiones de OS, nombres de servidores o modelos de hardware) que pueda ser utilizada para el reconocimiento por parte de un atacante. Se deben utilizar mensajes legales de "Acceso Restringido".

4. Procedimientos

4.1. Fase de Preparación y Selección de Baseline

Antes de configurar cualquier activo:

1. **Identificación del Activo:** El responsable técnico debe identificar el tipo de equipo (Switch, Router, Cámara IP, Centro de Impresión, etc.).
2. **Consulta de Estándar:** Se debe consultar la guía de configuración segura (Baseline) correspondiente a dicho activo. Si es un equipo nuevo sin estándar previo, el líder de TI definirá los parámetros mínimos basados en recomendaciones de fabricante o guías CIS.

4.2. Ejecución del Endurecimiento (Hardening)

El técnico asignado deberá aplicar los cambios directamente en el equipo siguiendo este orden:

1. **Aislamiento:** El equipo debe configurarse inicialmente en una red de laboratorio o fuera de la red de producción.

2. **Actualización:** Descargar e instalar la última versión estable del firmware o sistema operativo.
3. **Limpieza de Servicios:** Desactivar todos los servicios y puertos que no se utilicen (ej. desactivar Telnet en switches, desactivar el servicio de impresión inalámbrica si no se requiere, cerrar puertos USB).
4. **Aseguramiento de Acceso:** Cambiar contraseñas por defecto, renombrar usuarios administradores y configurar el tiempo de espera por inactividad (timeout).

4.3. Llenado del Registro de Hardening

Este es el paso crítico para la evidencia documental:

1. **Captura de Datos Técnicos:** Se registra en el formato el ID del activo, marca, modelo, versión de firmware y dirección IP asignada.
2. **Checklist de Configuración:** El técnico marca cada una de las acciones realizadas (ej. "Contraseña de fábrica cambiada: Sí", "Protocolos no cifrados desactivados: Sí").
3. **Validación de Sincronización:** Se debe confirmar en el registro que el equipo está apuntando al servidor NTP del Ayuntamiento (o al Directorio Activo) para la correcta sincronización de relojes.

4.4. Pruebas de Verificación (QA de Seguridad)

Una vez aplicado el hardening:

1. **Escaneo de Puertos:** Se realiza un escaneo rápido (ej. con Nmap) para verificar que solo los puertos declarados como necesarios están abiertos.
2. **Prueba de Acceso:** Intentar ingresar con las credenciales de fábrica para asegurar que el cambio fue efectivo.
3. **Firma de Conformidad:** Una vez superadas las pruebas, el técnico y el supervisor firman el **Registro de Hardening**.

4.5. Liberación a Producción e Inventario

1. **Conexión a Red:** Solo con el registro firmado, el equipo puede ser trasladado a su ubicación final y conectado a la red de producción.
2. **Resguardo de Evidencia:** El formato original se archiva (física o digitalmente) como parte de la evidencia del SGSI para futuras auditorías de la **ISO 27001**.
3. **Actualización de Inventario:** Se registra el activo en el inventario general con el estatus de "Endurecido/Seguro".

4.6. Auditoría de Mantenimiento (Re-Hardening)

1. **Revisión Periódica:** Semestralmente, se seleccionará una muestra aleatoria de equipos para verificar que su configuración no haya sido alterada.
2. **Actualización por Vulnerabilidades:** Si se detecta una vulnerabilidad crítica "Día Cero" que afecte a un equipo ya instalado, se debe repetir el procedimiento de hardening para aplicar el parche o mitigación necesaria y actualizar el registro.

5. Definiciones

- **Hardening (Endurecimiento):** Proceso de asegurar un sistema informático reduciendo su superficie de vulnerabilidad a través de la eliminación de funciones innecesarias y el refuerzo de controles de acceso.
- **Línea Base (Baseline):** Conjunto de parámetros de configuración mínima y obligatoria que debe cumplir un activo antes de ser considerado seguro para operar.
- **Superficie de Ataque:** Suma total de todos los puntos posibles (puertos, servicios, protocolos) donde un usuario no autorizado puede intentar introducir o extraer datos de un sistema.
- **CIS Benchmarks:** Estándares de configuración de seguridad desarrollados por el *Center for Internet Security*, reconocidos globalmente como las mejores prácticas para el endurecimiento de sistemas.
- **VLAN de Gestión:** Segmento de red aislado y restringido destinado exclusivamente a la administración técnica de los equipos de red y servidores, separada del tráfico de los usuarios.
- **Firmware:** Programa básico que controla los circuitos electrónicos de un dispositivo (como un router o una cámara); mantenerlo actualizado es vital para cerrar brechas de seguridad físicas.

6. Formatos

Para que el proceso de Hardening sea rastreable y cumpla con los requisitos de evidencia de la **ISO 27001**, se utilizará el siguiente registro maestro:

1. **F-HAR-01: Registro de Hardening de Activos**

7. Relación Normativa (ISO 27001:2022)

Este documento es el sustento técnico para los siguientes controles de la norma internacional:

Control	Título	Justificación del Cumplimiento
8.9	**Gestión de la configuración**	Establece el proceso para definir, documentar, monitorear y revisar las configuraciones de seguridad de todos los activos.
8.8	**Gestión de vulnerabilidades técnicas**	El hardening preventivo y el parcheo de firmware reducen las debilidades explotables en el hardware.
8.12	**Seguridad de los servicios de red**	Asegura que los switches, routers y módems estén configurados para resistir ataques externos.
8.1	**Dispositivos de usuario final**	Aplica las reglas de endurecimiento a laptops y PCs para proteger el punto final de la red.