Tabla de contenido

1. Propósito

Establecer los lineamientos y procedimientos para la identificación, evaluación y tratamiento de las vulnerabilidades técnicas en los activos de información del **H. Ayuntamiento de Morelia**.

Este documento busca:

- **Reducir la Superficie de Ataque:** Identificar debilidades en sistemas operativos, aplicaciones y hardware antes de que sean explotadas.
- **Priorización de Riesgos:** Clasificar las vulnerabilidades según su criticidad para optimizar el uso de los recursos de TI.
- **Mantener la Integridad y Disponibilidad:** Evitar interrupciones de servicios ciudadanos causadas por fallos de seguridad conocidos.
- **Garantizar el Cumplimiento:** Asegurar que todos los sistemas cuenten con las actualizaciones de seguridad necesarias para cumplir con los estándares internacionales.

2. Alcance

Esta política es aplicable a todos los activos tecnológicos propiedad o bajo custodia del Ayuntamiento, incluyendo:

- **Infraestructura de Red:** Firewalls, switches, routers y puntos de acceso.
- **Servidores:** Físicos y virtuales, tanto en sitio como en la nube.
- **Estaciones de Trabajo:** Laptops y computadoras de escritorio institucionales.
- **Aplicaciones y Bases de Datos:** Sistemas desarrollados internamente y software de terceros.
- **Dispositivos Móviles:** Enrolados en los sistemas de gestión institucional.

Agencia de la Ciudad Inteligente y Transformación Digital
H. Ayuntamiento de Morelia

3. Políticas de Gestión de Vulnerabilidades Técnicas

3.1. Estrategia de Gestión Proactiva

El Ayuntamiento adopta una postura de "vigilancia técnica continua". Se establece que la gestión de vulnerabilidades no es una actividad aislada, sino un ciclo recurrente de identificación, análisis, priorización y remediación. El objetivo primordial es minimizar la ventana de oportunidad para un atacante, manteniendo el inventario de software y firmware en las versiones estables más recientes que cuenten con soporte del fabricante.

3.2. Ejecución de Análisis de Vulnerabilidades (Vulnerability Scanning)

Se realizarán escaneos automatizados para identificar debilidades conocidas en la infraestructura:

- **Escaneos Internos:** Se ejecutarán de forma mensual sobre servidores críticos y trimestral sobre el resto de la red interna, buscando configuraciones deficientes o parches faltantes.
- **Escaneos Externos:** Se realizarán de forma mensual sobre todas las direcciones IP públicas y servicios expuestos a Internet (Portales ciudadanos, trámites en línea, VPN).
- **Escaneos tras Cambios Significativos:** Es obligatorio realizar un escaneo de vulnerabilidades inmediatamente después de cualquier cambio mayor en la red, actualización de base de datos o migración de servidores.

3.3. Realización de Pruebas de Penetración (Pentest)

A diferencia del escaneo automatizado, el Ayuntamiento implementará **Pruebas de Penetración** para simular ataques reales y evaluar la eficacia de los controles de detección:

- **Periodicidad:** Se llevará a cabo al menos un Pentest integral de "Caja Negra" o "Caja Gris" cada vez que se libere un sistema de desarrollo propio con impacto en la ciudadanía. Posteriormente deberá realizarse anualmente por parte de un tercero.
- **Alcance del Pentest:** Las pruebas deben incluir, como mínimo, el análisis de la red perimetral, aplicaciones web y la configuración de seguridad del Directorio Activo.
- **Validación de Hallazgos:** No se dará por corregida una vulnerabilidad crítica hasta que una prueba de penetración dirigida (Retest) confirme que el vector de ataque ha sido mitigado efectivamente.

3.4. Herramientas Autorizadas y Uso de Software Open Source

Para democratizar la seguridad y optimizar el presupuesto institucional, el Ayuntamiento permite y fomenta el uso de herramientas tanto comerciales como de código abierto (Open Source), siempre que sean ejecutadas por personal capacitado y bajo entornos controlados:

- **Análisis de Aplicaciones Web:** Se autoriza el uso de **OWASP ZAP** y **Burp Suite** para identificar vulnerabilidades tipo SQL Injection, Cross-Site Scripting (XSS) y debilidades en la autenticación.
- **Gestión de Vulnerabilidades de Infraestructura:** Se permite el uso de soluciones de alto nivel como **InsightVM (Rapid7)**, así como herramientas robustas de diagnóstico como **Nmap**, **OpenVAS** o el motor de búsqueda de parches de **Bitdefender**.

- **Cumplimiento y Licenciamiento:** El uso de herramientas Open Source no exime al personal de la responsabilidad de mantener las herramientas actualizadas y de asegurar que el tráfico generado durante las pruebas no degrade los servicios públicos.

3.5. Clasificación y Priorización bajo el Estándar CVSS

Toda vulnerabilidad hallada será categorizada utilizando el sistema de puntuación **CVSS (Common Vulnerability Scoring System)** en su versión más reciente. Los tiempos de respuesta obligatorios son:

- **Nivel Crítico (9.0 - 10.0):** Requiere atención inmediata. Tiempo de remediación o aplicación de control compensatorio: **Máximo 48 horas**.
- **Nivel Alto (7.0 - 8.9):** Requiere remediación prioritaria. Tiempo máximo: **10 días hábiles**.
- **Nivel Medio (4.0 - 6.9):** Se atenderá en la ventana de mantenimiento mensual programada.
- **Nivel Bajo (0.1 - 3.9):** Se monitorea y se corrige según la disponibilidad operativa.

3.6. Seguridad en el Ciclo de Desarrollo y Pre-producción

Queda estrictamente prohibido el paso a producción de cualquier sistema, aplicación o módulo desarrollado internamente o por terceros que presente vulnerabilidades de nivel **Alto** o **Crítico**. Antes de cualquier despliegue, el área de TI debe emitir un "Sello de Aptitud Técnica" basado en un escaneo de vulnerabilidades limpio.

3.7. Gestión de Riesgos en Sistemas Heredados (Legacy)

En el caso de sistemas que no admitan parches de seguridad por su antigüedad, pero que sean vitales para la operación del Ayuntamiento:

- Se debe documentar una **Excepción de Seguridad** firmada por el titular del área.
- Se implementarán **Controles Compensatorios** obligatorios, tales como el aislamiento del equipo en una VLAN sin acceso a Internet, endurecimiento del firewall (Virtual Patching) o el uso de listas blancas de aplicaciones.

3.8. Verificación de Post-Remediación

Todo parche aplicado o cambio de configuración realizado como resultado de esta política debe ser validado técnicamente. La evidencia del "Antes" y "Después" es requisito indispensable para dar cumplimiento a las auditorías de la norma ISO 27001.

4. Procedimientos

4.1. Detección y Escaneo Automatizado de Infraestructura

El proceso inicia con la ejecución de escaneos programados desde la consola de **InsightVM** o el módulo de parches de **Bitdefender**. El personal técnico debe configurar perfiles de escaneo que cubran tanto los segmentos de red interna (servidores y estaciones de trabajo) como los perímetros externos (IPs públicas).

En el caso de activos nuevos o de reciente incorporación, se debe realizar un escaneo de descubrimiento mediante **Nmap** para identificar puertos abiertos y servicios activos antes de proceder con el análisis de vulnerabilidades profundo. Los resultados de estos escaneos se consolidan en un informe técnico bruto que servirá de base para el análisis.

4.2. Análisis de Resultados, Triaje y Validación de Falsos Positivos

Una vez obtenido el informe bruto, el analista de seguridad debe filtrar los hallazgos para descartar falsos positivos. Para ello, se contrastará la versión del software reportada con la configuración real del sistema.

Se aplicará el criterio de **contextualización**: si una vulnerabilidad es reportada en un servicio que, aunque esté instalado, se encuentra deshabilitado o protegido por una regla estricta de firewall perimetral, su prioridad puede ser ajustada. El resultado final de este procedimiento es una lista depurada de vulnerabilidades reales, priorizadas por su puntaje **CVSS** y su impacto en la continuidad de los servicios del Ayuntamiento.

4.3. Ejecución de Pruebas de Penetración (Pentesting) en Aplicaciones Web

Para los portales ciudadanos y aplicaciones de trámites, se ejecutará un procedimiento de explotación controlada utilizando **OWASP ZAP** o **Burp Suite**.

- **Fase de Exploración:** La herramienta realiza un mapeo de la estructura del sitio y las entradas de datos.
- **Ataque Controlado:** Se lanzan vectores de ataque para identificar fallos de tipo SQL Injection, XSS o debilidades en la gestión de sesiones.
- **Documentación de Hallazgos:** Cada vulnerabilidad encontrada debe ser documentada con una captura de pantalla (evidencia) y una descripción del impacto potencial, permitiendo que el equipo de desarrollo comprenda el fallo exacto.

4.4. Planificación y Pruebas de Remediación en Entornos Controlados

Antes de aplicar parches de seguridad de forma masiva, especialmente en servidores críticos (Tesorería, Catastro), se debe seleccionar un "Grupo de Control" o un entorno de pre-producción. Se aplican las actualizaciones o cambios de configuración y se verifica la estabilidad del sistema durante un periodo de 24 a 48 horas.

Si no se detectan degradaciones en el servicio o conflictos con las aplicaciones institucionales, se genera la orden de despliegue general. En caso de falla, se debe documentar el error y buscar una medida compensatoria alternativa.

4.5. Despliegue de Remediación y Parchado (Patch Management)

El despliegue se realiza de forma centralizada. Para estaciones de trabajo y laptops, se utiliza la consola de administración para empujar los parches de seguridad. Para equipos de red (switches, firewalls), el procedimiento requiere una ventana de mantenimiento programada donde se realiza la actualización del firmware de forma manual o asistida.

En situaciones de **Vulnerabilidades Críticas (Día Cero)**, se omite la ventana de mantenimiento y se procede al parchado de emergencia previa autorización del Director de TI, notificando a las áreas usuarias sobre la breve interrupción del servicio.

4.6. Verificación de Cierre y Re-escaneo (Retesting)

Este es el paso de control de calidad. Una vez que el equipo técnico reporta la remediación, se debe ejecutar un **re-escaneo dirigido** exclusivamente a los activos y vulnerabilidades tratadas.

- Si la herramienta de escaneo confirma que la vulnerabilidad ha desaparecido, se marca el hallazgo como **"Cerrado"**.

- Si la vulnerabilidad persiste, se escala el incidente para una revisión manual profunda.

La evidencia del escaneo de verificación es el documento primordial para demostrar el cumplimiento del control **8.8**ante un auditor de la ISO 27001.

4.7. Gestión de Excepciones y Riesgo Aceptado

En activos donde la remediación técnica sea imposible (ej. software legacy que deja de funcionar con el parche), se seguirá el procedimiento de excepción:

1. **Justificación:** El titular del área explica por qué no se puede aplicar el parche.
2. **Control Compensatorio:** TI configura medidas de aislamiento (VLANs, endurecimiento de Firewall).
3. **Formalización:** Se firma el formato de **Aceptación de Riesgo**, el cual debe renovarse anualmente o cada que cambie el panorama de amenazas.

5. Definiciones

- **CVE (Common Vulnerabilities and Exposures):** Un catálogo de vulnerabilidades de seguridad informática de conocimiento público. Cada registro tiene un número único (ej. CVE-2024-XXXX) que permite a los técnicos identificar fallos específicos.
- **CVSS (Common Vulnerability Scoring System):** Sistema de puntuación estándar (de 0 a 10) que mide la severidad de una vulnerabilidad basándose en criterios como la facilidad de explotación y el impacto en la información.
- **Exploit:** Fragmento de software, datos o secuencia de comandos que aprovecha una vulnerabilidad para provocar un comportamiento no deseado en un sistema (como el acceso no autorizado).
- **Falso Positivo:** Resultado de un escaneo que indica la presencia de una vulnerabilidad que en realidad no existe o que ya ha sido mitigada por otros medios.
- **Pentesting (Prueba de Penetración):** Práctica de simular un ataque contra un sistema informático para encontrar vulnerabilidades que un atacante podría explotar.
- **Vulnerabilidad de Día Cero (Zero-Day):** Un fallo de seguridad recién descubierto para el cual el fabricante aún no ha lanzado un parche de remediación.

6. Formatos

Para que el ciclo de vida de la vulnerabilidad sea auditable, utilizaremos los siguientes registros:

- **F-GV-01: Reporte Técnico de Vulnerabilidades y Pentest**
  - *Uso:* Documento que consolida los hallazgos de herramientas como **InsightVM** o **OWASP ZAP**, incluyendo capturas de pantalla y el puntaje CVSS.
- **F-GV-02: Bitácora de Remediación y Validación de Parches**
  - *Uso:* Control donde se registra la fecha de aplicación del parche, el ID del equipo y el resultado del re-escaneo de validación.
- **F-GV-03: Formato de Excepción de Seguridad y Aceptación de Riesgo**
  - *Uso:* Documento legal-técnico para sistemas *legacy* o críticos que no pueden ser parchados, firmado por el titular de la dependencia responsable.
- **F-GV-04: Sello de Aptitud Técnica (Pre-producción)**
  - *Uso:* Autorización firmada por TI para que un nuevo desarrollo o sistema pueda ser publicado en internet tras pasar un escaneo limpio.

7. Relación con Requisitos Normativos (ISO 27001:2022)

Este documento es el corazón del cumplimiento técnico y se vincula directamente con los siguientes controles del Anexo A:

Control Anexo A	Título del Control	Descripción del Cumplimiento
8.8	**Gestión de vulnerabilidades técnicas**	**Control Principal:** Se cumple mediante el ciclo de detección, priorización CVSS y remediación obligatoria.
8.19	**Instalación de software en sistemas operativos**	Se asegura que la actualización de sistemas sea un proceso controlado y probado antes de su despliegue masivo.
5.7	**Inteligencia de Amenazas**	La política obliga a usar la información de amenazas externas para disparar escaneos de emergencia.

Control Anexo A	Título del Control	Descripción del Cumplimiento
8.29	**Seguridad en las pruebas**	Se garantiza que el uso de herramientas como **Burp Suite** o **Nmap** se realice bajo condiciones que no afecten la operación real.

Agencia de la Ciudad Inteligente y Transformación Digital
H. Ayuntamiento de Morelia