Tabla de contenido

1. Propósito

El propósito de este documento es establecer los lineamientos y controles técnicos para la prevención, detección y respuesta ante software malicioso (malware) dentro de la infraestructura tecnológica del **H. Ayuntamiento de Morelia**.

A través de esta política, se busca garantizar la integridad y disponibilidad de la información institucional mediante:

- **Protección Preventiva:** Asegurar que todos los activos tecnológicos cuenten con defensas activas antes de interactuar con redes externas o medios extraíbles.
- **Detección Temprana:** Implementar mecanismos de monitoreo centralizado que permitan identificar intentos de infección o comportamientos anómalos de forma inmediata.
- **Respuesta Eficaz:** Definir protocolos de contención para evitar que un brote de malware se propague lateralmente por la red institucional.
- **Cultura de Uso Seguro:** Fomentar prácticas responsables en los colaboradores para minimizar los vectores de entrada de código malicioso.

2. Alcance

Esta política es de cumplimiento obligatorio para todo el personal que utilice recursos tecnológicos del Ayuntamiento y cubre todos los activos de información conectados a la red institucional o que procesen datos oficiales:

2.1. Activos Cubiertos

- **Servidores:** Físicos y virtuales, independientemente del sistema operativo (Windows Server, Linux).
- **Estaciones de Trabajo y Laptops:** Equipos de oficina y dispositivos móviles asignados para trabajo remoto.
- **Dispositivos Móviles:** Smartphones y tabletas institucionales o personales vinculadas mediante esquemas de gestión móvil.
- **Servicios de Correo:** Protección a nivel de buzón para filtrado de adjuntos y enlaces maliciosos.

2.2. Infraestructura de Gestión

- **Consola Centralizada:** Se establece el uso de la consola central de administración (ej. Bitdefender GravityZone) como el único punto de control, despliegue y monitoreo oficial para el cumplimiento de esta política.

3. Políticas de Gestión de Antimalware

3.1. Obligatoriedad y Despliegue

- **Instalación Universal:** Todo activo tecnológico que se conecte a la red institucional o procese información del Ayuntamiento debe tener instalado el agente antimalware oficial. No se permite la operación de equipos con soluciones "gratuitas", de prueba o versiones de consumo personal.
- **Estado de Protección Activa:** La protección en tiempo real (Real-time Scanning) debe estar habilitada permanentemente. Bajo ninguna circunstancia se permite el procesamiento de datos en equipos con el motor de búsqueda desactivado.

3.2. Administración y Control Centralizado

- **Gestión vía Consola:** La configuración, actualización y monitoreo de las amenazas se realizará exclusivamente a través de la **consola central de administración**. Se prohíben las instalaciones "stand-alone" (aisladas) que no reporten al centro de control.
- **Restricción de Privilegios al Usuario:** Queda estrictamente prohibido que el usuario final desactive, pause o modifique la configuración del software antimalware.
- **Protección contra Desinstalación:** El agente deberá contar con una contraseña de desinstalación o protección de manipulación (*Tamper Protection*) custodiada únicamente por la Dirección de TI.

3.3. Gestión de Firmas y Actualizaciones

- **Automatización de Updates:** El agente debe estar configurado para buscar y descargar actualizaciones de firmas y parches de seguridad de forma automática.
- **Frecuencia de Actualización:** En equipos con conexión permanente, las firmas deben actualizarse al menos cada 4 horas. Para equipos móviles, la actualización se ejecutará inmediatamente al detectar conexión a internet.

3.4. Control de Medios Extraíbles y Dispositivos Externos

- **Escaneo Automático:** Se establece como obligatorio el escaneo automático de cualquier medio de almacenamiento extraíble (USB, discos duros externos, tarjetas SD) al momento de ser insertado en un equipo institucional.

- **Bloqueo por Incumplimiento:** En áreas de alta criticidad (Tesorería, SITE, Archivo), TI podrá implementar el bloqueo total de puertos USB, permitiendo únicamente el uso de dispositivos autorizados y previamente analizados.

3.5. Análisis y Escaneos Programados

- **Análisis Completo (Full Scan):** Se debe programar un análisis completo de todos los archivos del sistema al menos una vez por semana, preferentemente en horarios de baja carga operativa.
- **Análisis Crítico:** Se ejecutará un análisis de áreas críticas (memoria, sectores de arranque, archivos temporales) diariamente al iniciar la jornada laboral.

3.6. Manejo de Hallazgos y Amenazas

- **Cuarentena Automática:** Toda amenaza detectada debe ser movida a una zona de cuarentena segura de forma inmediata, impidiendo su ejecución.
- **Notificación de Incidentes:** La consola debe estar configurada para enviar alertas automáticas al personal de TI ante detecciones críticas o brotes masivos que sugieran un intento de movimiento lateral (tipo Ransomware).

4. Procedimientos

4.1. Despliegue e Instalación del Agente de Protección

El ciclo de protección inicia con el aseguramiento del equipo terminal. El administrador de TI realiza el descubrimiento de activos dentro de la red institucional para identificar dispositivos sin protección activa. Una vez localizado el equipo, se ejecuta el despliegue remoto del paquete de instalación preconfigurado desde la consola central.

Al finalizar la transferencia, se verifica que el dispositivo aparezca con estado "Protegido" y con el motor de búsqueda actualizado en el tablero de control. En caso de falla en la instalación remota, se procede con una instalación local manual, asegurando siempre que el equipo quede vinculado al inventario digital de la consola antes de entregar el activo al usuario final.

4.2. Monitoreo Diario y Gestión de Alertas

El personal técnico responsable debe realizar una revisión diaria de la consola de administración durante la primera hora de la jornada laboral. Esta supervisión se enfoca en identificar tres escenarios críticos:

- **Equipos Desactualizados:** Dispositivos que no hayan descargado firmas en las últimas 24 horas.
- **Agentes Inactivos:** Equipos que no han reportado comunicación con la consola en los últimos 7 días.
- **Amenazas no Neutralizadas:** Detecciones que el motor automático no pudo mover a cuarentena o eliminar por sí solo.

Ante cualquier anomalía detectada en estos rubros, se inicia una tarea de remediación remota forzada desde la consola.

4.3. Respuesta y Contención ante Detección de Amenazas

Al dispararse una alerta de infección de alta criticidad, se activa de inmediato el protocolo de aislamiento. El administrador de TI utiliza las capacidades de la consola para **aislar lógicamente el equipo de la red**, permitiendo únicamente la comunicación entre el agente y el servidor de seguridad para evitar la propagación lateral del código malicioso.

Posteriormente, se ejecuta un análisis profundo de todo el sistema y se revisan los registros de ejecución para identificar el origen de la entrada (ej. correo electrónico, USB o navegación). Una vez confirmada la limpieza total del sistema y eliminados los archivos temporales de riesgo, se restaura la conectividad del equipo a la red institucional.

4.4. Gestión de Exclusiones y Falsos Positivos

En situaciones donde el software de seguridad interfiera con el rendimiento de aplicaciones críticas del Ayuntamiento, el titular de la dependencia afectada debe solicitar formalmente una exclusión. El área de TI analiza el riesgo y, de ser viable, configura la exclusión específicamente para la ruta o el proceso necesario, evitando exclusiones genéricas o masivas que debiliten la seguridad.

Todas las exclusiones aplicadas deben ser revisadas trimestralmente para validar si siguen siendo necesarias o si el software en cuestión ha sido actualizado para coexistir con el antimalware.

4.5. Tratamiento de Medios Extraíbles

El procedimiento de análisis de dispositivos USB es automático y obligatorio. Al insertar un medio externo, el agente bloquea el acceso a los archivos hasta que se complete un escaneo rápido de los sectores de arranque y archivos raíz. Si se detecta malware, el dispositivo es bloqueado por completo y se notifica al usuario que el medio debe ser formateado o entregado a TI para su desinfección profunda bajo entornos controlados.

4.6. Mantenimiento y Depuración de la Consola

De manera mensual, se realiza una depuración de la base de datos de la consola. Se eliminan los registros de equipos que han sido dados de baja patrimonial o que han cambiado de nombre de host, asegurando que las métricas de cumplimiento y los reportes de salud de la red reflejen la realidad operativa de las dependencias.

5. Definiciones

- **Aislamiento de Red (Network Isolation):** Capacidad técnica de la consola para cortar toda comunicación de un equipo infectado con el resto de la red, manteniendo solo el enlace con el servidor de administración para tareas de limpieza.
- **Consola de Administración Centralizada:** Plataforma única (ej. Bitdefender GravityZone) desde la cual se gestionan las políticas, actualizaciones y alertas de todos los endpoints de la institución.
- **Endpoint:** Cualquier dispositivo informático que actúa como punto final en una red, tales como estaciones de trabajo, laptops, servidores o dispositivos móviles.
- **Falso Positivo:** Alerta generada por el software de seguridad al identificar erróneamente un archivo o proceso legítimo como malicioso.
- **Firmas de Virus (Definitions):** Base de datos que contiene las huellas digitales de malware conocido, utilizada por el motor de búsqueda para identificar amenazas.
- **Movimiento Lateral:** Técnica utilizada por el malware (especialmente el Ransomware) para propagarse desde un equipo infectado a otros servidores o estaciones dentro de la misma red.
- **Protección en Tiempo Real:** Proceso de monitoreo constante que analiza archivos y programas en el momento exacto en que son abiertos, ejecutados o creados.

H. Ayuntamiento de Morelia

6. Formatos

Para que la gestión sea auditable y se genere la evidencia necesaria para el SGSI, se establecen los siguientes registros:

- **F-AM-01: Reporte Ejecutivo Mensual de Salud y Amenazas**
  - *Uso:* Informe generado desde la consola que detalla el porcentaje de equipos protegidos, volumen de amenazas detectadas y efectividad de la limpieza.
- **F-AM-02: Registro de Exclusiones de Seguridad**
  - *Uso:* Bitácora donde se documenta la justificación técnica de por qué un archivo o carpeta ha sido omitido del escaneo, con firma de autorización del responsable de TI.
- **F-AM-03: Bitácora de Incidentes y Desinfección Profunda**
  - *Uso:* Documento técnico donde se narra el origen de una infección masiva, las acciones de contención tomadas y la validación final de limpieza.
- **F-AM-04: Inventario de Dispositivos No Reportados**
  - *Uso:* Control de seguimiento para equipos que han perdido conexión con la consola y requieren intervención física.

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

Este documento atiende específicamente los siguientes controles del Anexo A, asegurando que el Ayuntamiento pase cualquier auditoría de cumplimiento técnico:

Control Anexo A	Título del Control	Descripción del Cumplimiento
8.7	**Protección contra malware**	Se cumple íntegramente mediante la política de instalación obligatoria, protección en tiempo real y escaneo de medios extraíbles.
8.1	**Dispositivos de usuario final**	Se garantiza que todo equipo de usuario esté bajo el control de la consola central antes de su entrega.
8.16	**Seguimiento de eventos**	La consola central actúa como el registro maestro de eventos de seguridad (logs) relacionados con código malicioso.

H. Ayuntamiento de Morelia

Control Anexo A	Título del Control	Descripción del Cumplimiento
5.28	**Recopilación de evidencia digital**	Los reportes de la consola y las bitácoras de desinfección sirven como evidencia técnica en caso de investigaciones forenses.
8.19	**Instalación de software en sistemas operativos**	Se restringe la capacidad del usuario de deshabilitar protecciones para instalar software no autorizado.

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