Tabla de contenido

H. Ayuntamiento de Morelia

1. Propósito

El presente documento tiene como objetivo establecer el marco operativo para la recopilación, análisis y aplicación de información sobre amenazas de seguridad de la información.

A través de la Inteligencia de Amenazas, buscamos:

- **Anticipación Proactiva:** Identificar tendencias de ataques y nuevas vulnerabilidades antes de que afecten la infraestructura municipal.
- **Toma de Decisiones Informada:** Proveer datos accionables a la Dirección de TI para priorizar inversiones y cambios en la configuración de seguridad.

El presente documento es de carácter confidencial de uso controlado, por lo que está prohibida su reproducción parcial o total para uso externo. Si un ejemplar impreso de este documento no tiene las firmas del control de emisión, se trata de una copia no controlada. Consulte nuestro aviso de privacidad en https://contraloria.morelia.gob.mx/contraloria/aviso-de-privacidad

- **Optimización de la Respuesta:** Reducir los tiempos de detección mediante el uso de Indicadores de Compromiso (IoCs) actualizados.
- **Concientización Focalizada:** Informar al personal sobre campañas específicas de phishing o ingeniería social dirigidas al sector gubernamental.

2. Alcance

Esta política aplica a todos los niveles de la Dirección de TI y áreas estratégicas del Ayuntamiento que tengan la capacidad de modificar controles de seguridad o tomar decisiones basadas en riesgos. Cubre información de fuentes externas (proveedores, gobierno, comunidades de ciberseguridad) e internas (análisis de incidentes propios).

3. Políticas de Inteligencia de Amenazas

3.1. Cultura de Vigilancia e Información Continua

Se establece como una **prioridad estratégica** para el personal de ciberseguridad y alta dirección el mantenerse informado sobre el panorama de riesgos digitales.

- **Vitalidad de la Información:** El Ayuntamiento reconoce que una postura defensiva estática es insuficiente. Es obligatorio dedicar tiempo de la jornada técnica a la consulta de fuentes de inteligencia para anticipar vectores de ataque antes de que se manifiesten en la infraestructura local.
- **Superación del Ruido Informativo:** La política prohíbe la simple acumulación pasiva de noticias. La información consultada debe ser digerida y analizada para determinar su relevancia técnica y operativa para las dependencias municipales.

3.2. Vinculación con Grupos de Interés Especial (Enlace Normativo 5.6)

La inteligencia de amenazas se nutre del intercambio colaborativo. Por ello, la Dirección de TI debe mantener una comunicación activa y bidireccional con organismos especializados:

- **Organismos Oficiales:** Es mandatorio el contacto y seguimiento de los boletines emitidos por el **CERT-MX**, la **Guardia Nacional (Dirección General de Científica)** y el **Centro Nacional de Inteligencia (CNI)**.
- **Comunidades de Ciberseguridad:** Se fomentará la participación en foros, grupos de respuesta a incidentes y asociaciones de profesionales de seguridad (como

El presente documento es de carácter confidencial de uso controlado, por lo que está prohibida su reproducción parcial o total para uso externo. Si un ejemplar impreso de este documento no tiene las firmas del control de emisión, se trata de una copia no controlada. Consulte nuestro aviso de privacidad en https://contraloria.morelia.gob.mx/contraloria/aviso-de-privacidad

ISACA, ISC², o grupos regionales de Jalisco y Michoacán) para conocer de primera mano las amenazas que están afectando al sector público en México.
- **Relación con Proveedores:** Se debe explotar la inteligencia táctica provista por los fabricantes de las herramientas actuales (ej. la telemetría global de **Bitdefender**), asegurando que las alertas de "día cero" sean atendidas con prioridad máxima.

3.3. Criterios de Calidad y Relevancia de la Inteligencia

Para que la información sea considerada "Inteligencia de Amenazas" dentro del SGSI, debe cumplir con tres atributos:

1. **Pertinencia:** Debe estar relacionada directamente con las tecnologías, software y activos que utiliza el Ayuntamiento (ej. si sale una vulnerabilidad de un software que no usamos, se descarta).
2. **Oportunidad:** La información debe ser recibida y procesada en un tiempo que permita la acción preventiva; una noticia de hace un mes no es inteligencia, es historia.
3. **Accionabilidad:** Toda información de inteligencia debe tener el potencial de convertirse en un cambio de configuración, una regla de bloqueo o un parche de seguridad.

3.4. Confidencialidad en el Intercambio de Información

Al colaborar con grupos de interés o dependencias pares, el personal del Ayuntamiento debe observar estrictas reglas de confidencialidad:

- **Protocolo de Semáforo (TLP):** Se adoptará el uso del *Traffic Light Protocol* (Rojo, Ámbar, Verde, Blanco) para el intercambio de información, asegurando que los datos sensibles sobre las vulnerabilidades propias del Ayuntamiento no sean divulgados más allá de los círculos autorizados.
- **Anonimización:** Antes de compartir indicadores de ataques sufridos internamente, se deberán eliminar datos que identifiquen específicamente a la dependencia o a los usuarios afectados, a menos que sea estrictamente necesario para la mitigación coordinada.

3.5. Institucionalización de la Inteligencia

La inteligencia de amenazas no debe ser un conocimiento aislado de un solo técnico. Los hallazgos más críticos deben ser documentados en la **Matriz de Riesgos** del

El presente documento es de carácter confidencial de uso controlado, por lo que está prohibida su reproducción parcial o total para uso externo. Si un ejemplar impreso de este documento no tiene las firmas del control de emisión, se trata de una copia no controlada. Consulte nuestro aviso de privacidad en https://contraloria.morelia.gob.mx/contraloria/aviso-de-privacidad

H. Ayuntamiento de Morelia

Ayuntamiento, permitiendo que la alta dirección entienda por qué se están tomando ciertas decisiones presupuestales o cambios de arquitectura.

4. Procedimientos

4.1. Establecimiento de Enlaces y Suscripción a Fuentes de Inteligencia

El proceso inicia con la formalización de la red de contactos y fuentes. El enlace técnico de seguridad de la Dirección de TI debe realizar la suscripción oficial de las cuentas de correo institucionales a los servicios de alerta temprana del **CERT-MX**, la **Guardia Nacional** y el **CNI**.

Simultáneamente, se debe establecer un canal de comunicación (vía correo o plataformas de mensajería segura) con grupos de interés especial y dependencias gubernamentales pares. El registro de estos contactos debe mantenerse actualizado en la base de datos de "Grupos de Interés Especial", asegurando que el Ayuntamiento reciba boletines de vulnerabilidades de día cero y tendencias de ataques dirigidos al sector público de forma inmediata.

4.2. Monitoreo Diario y Recolección de Datos

Durante la primera hora de la jornada laboral, el personal designado realizará una ronda de vigilancia digital. Esta actividad consiste en revisar la telemetría global de la consola de **Bitdefender** para identificar tendencias mundiales, así como la consulta de los boletines de vulnerabilidades (**CVE**) publicados en las últimas 24 horas.

H. Ayuntamiento de Morelia

Durante este monitoreo, se deben extraer los **Indicadores de Compromiso (IoCs)**, tales como direcciones IP maliciosas, nombres de dominio fraudulentos y *hashes* de archivos relacionados con campañas de Ransomware o Phishing activas en territorio nacional.

4.3. Triaje y Análisis de Relevancia Institucional

Toda la información recolectada debe pasar por un filtro de pertinencia técnica. El analista debe contrastar las amenazas detectadas contra el **Inventario de Activos** del Ayuntamiento. Si una vulnerabilidad reportada afecta a un software, sistema operativo o hardware que no está presente en la infraestructura municipal, se archiva como "Información de Contexto".

El presente documento es de carácter confidencial de uso controlado, por lo que está prohibida su reproducción parcial o total para uso externo. Si un ejemplar impreso de este documento no tiene las firmas del control de emisión, se trata de una copia no controlada. Consulte nuestro aviso de privacidad en https://contraloria.morelia.gob.mx/contraloria/aviso-de-privacidad

Si la amenaza es pertinente, se procede a determinar su nivel de criticidad basándose en el impacto potencial a los servicios ciudadanos y la facilidad de explotación. Este análisis debe generar un breve diagnóstico que responda: *¿Qué activo está en riesgo?* y *¿Qué control actual nos protege?*

4.4. Accionabilidad y Mitigación Preventiva

Una vez confirmada la relevancia, la inteligencia se traduce en acciones técnicas de endurecimiento:

- **Bloqueo Perimetral:** Las IPs y dominios identificados como maliciosos se cargan de inmediato en las reglas de filtrado del Firewall institucional.
- **Actualización de Listas Negras:** Los *hashes* de archivos maliciosos se agregan a la lista de bloqueo de la consola de **Bitdefender** para evitar su ejecución en cualquier endpoint.
- **Parchado de Emergencia:** Si la inteligencia advierte sobre una vulnerabilidad crítica que está siendo explotada activamente ("In the wild"), se dispara el procedimiento de gestión de vulnerabilidades para aplicar el parche de seguridad de forma prioritaria, sin esperar a la ventana de mantenimiento mensual.

4.5. Comunicación y Difusión bajo Protocolo TLP

Para el intercambio de información con los grupos de interés, se aplicará estrictamente el **Traffic Light Protocol (TLP)**:

- **TLP:RED:** Información para ojos internos únicamente (ej. detalles de una vulnerabilidad propia).
- **TLP:AMBER:** Información para compartir solo con áreas técnicas internas y socios de confianza que necesiten saberla para protegerse.
- **TLP:GREEN:** Información para compartir con la comunidad de ciberseguridad y dependencias pares.
- **TLP:CLEAR:** Información pública.

En caso de que el Ayuntamiento detecte un nuevo vector de ataque, se enviará un reporte anonimizado a los grupos de interés correspondientes para alertar a la comunidad, cumpliendo así con la responsabilidad de colaboración interinstitucional.

H. Ayuntamiento de Morelia

El presente documento es de carácter confidencial de uso controlado, por lo que está prohibida su reproducción parcial o total para uso externo. Si un ejemplar impreso de este documento no tiene las firmas del control de emisión, se trata de una copia no controlada. Consulte nuestro aviso de privacidad en https://contraloria.morelia.gob.mx/contraloria/aviso-de-privacidad

4.6. Producción de Reportes de Inteligencia Estratégica

Semanalmente, se sintetizará la información técnica en un reporte ejecutivo de una página destinado a la alta dirección. Este documento debe evitar tecnicismos innecesarios y enfocarse en el "Panorama de Riesgo": qué amenazas están creciendo, cómo se ha protegido el Ayuntamiento preventivamente y si se requiere alguna inversión o cambio de política para hacer frente a las nuevas tendencias.

5. Definiciones

- **CERT (Computer Emergency Response Team):** Equipo de expertos responsable de responder a incidentes de seguridad. En México, el **CERT-MX** es la autoridad máxima para el sector público.
- **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).
- **IoC (Indicadores de Compromiso):** Datos forenses (direcciones IP, nombres de dominio o hashes de archivos) que indican con alta probabilidad que un sistema ha sido infiltrado.
- **TLP (Traffic Light Protocol):** Un conjunto de etiquetas utilizadas para designar con quién se puede compartir información sensible.
- **Vulnerabilidad de Día Cero (Zero-Day):** Una falla de seguridad en software o hardware que es desconocida para el fabricante y para la cual no existe un parche de seguridad disponible.

H. Ayuntamiento de Morelia

6. Formatos

Para que el auditor vea que realmente estás "haciendo la tarea" de inteligencia, utilizaremos estos registros:

- **F-IA-01: Registro de Grupos de Interés y Fuentes de Inteligencia**
  - *Uso:* Directorio de contactos en la Guardia Nacional, CERT-MX, y boletines a los que está suscrito el Ayuntamiento.
- **F-IA-02: Bitácora de Análisis y Acción de Inteligencia**
  - *Uso:* Registro donde se anota qué amenaza se detectó afuera y qué regla se cambió en el Firewall o en Bitdefender para prevenirla.
- **F-IA-03: Boletín de Alerta Técnica (Flash Report)**

El presente documento es de carácter confidencial de uso controlado, por lo que está prohibida su reproducción parcial o total para uso externo. Si un ejemplar impreso de este documento no tiene las firmas del control de emisión, se trata de una copia no controlada. Consulte nuestro aviso de privacidad en https://contraloria.morelia.gob.mx/contraloria/aviso-de-privacidad

  - *Uso:* Formato rápido para avisar a los técnicos de otras dependencias sobre una amenaza inminente.
- **F-IA-04: Reporte Semanal del Panorama de Amenazas**
  - *Uso:* Resumen ejecutivo para los titulares de las dependencias.

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

Este documento es el sustento principal para dos de los controles más estratégicos de la nueva versión de la norma:

Control	Título	Justificación del Cumplimiento
5.7	**Inteligencia de Amenazas**	Se cumple al establecer la recolección, análisis y transformación de datos externos en acciones de defensa.
5.6	**Contacto con grupos de interés especial**	Se materializa mediante el procedimiento de vinculación y comunicación con organismos como el CERT-MX y la Guardia Nacional.
8.8	**Gestión de vulnerabilidades técnicas**	La inteligencia de amenazas sirve como el disparador para priorizar el parchado de sistemas críticos.
5.25	**Evaluación y decisión sobre eventos de seguridad**	Provee el contexto necesario para que el equipo de TI sepa si un comportamiento extraño es un ataque nuevo o un error técnico.

H. Ayuntamiento de Morelia

El presente documento es de carácter confidencial de uso controlado, por lo que está prohibida su reproducción parcial o total para uso externo. Si un ejemplar impreso de este documento no tiene las firmas del control de emisión, se trata de una copia no controlada. Consulte nuestro aviso de privacidad en https://contraloria.morelia.gob.mx/contraloria/aviso-de-privacidad