Tabla de contenido

1. Propósito

El propósito de este documento es establecer un marco de respuesta estructurado para identificar, reportar, gestionar y aprender de los incidentes de seguridad de la información que afecten al **H. Ayuntamiento de Morelia**.

Se busca transformar la reacción caótica en una operación profesional que garantice:

- **Prontitud en la Respuesta:** Minimizar el tiempo transcurrido entre la detección de un evento y su mitigación.
- **Contención del Daño:** Evitar que un incidente menor (ej. un equipo infectado) se convierta en una crisis institucional (ej. caída de los servicios ciudadanos).
- **Recuperación Operativa:** Restablecer la normalidad de los procesos administrativos y servicios públicos en el menor tiempo posible.
- **Preservación de Evidencia:** Asegurar que los rastros digitales sean protegidos para posibles acciones legales o administrativas.
- **Mejora Continua:** Utilizar cada incidente como una lección aprendida para fortalecer los controles preventivos.

2. Alcance

Esta política es de cumplimiento obligatorio para todo el personal (base, confianza, honorarios y prestadores de servicio) del Ayuntamiento y aplica a todos los activos de información, servicios digitales e infraestructura física.

2.1. Clasificación de Eventos e Incidentes

- **Evento de Seguridad:** Cualquier ocurrencia identificada en un sistema o red que indica un posible fallo en la seguridad (ej. un log de acceso fallido).
- **Incidente de Seguridad:** Un evento o serie de eventos que tienen una probabilidad significativa de comprometer las operaciones institucionales o amenazar la seguridad de la información (ej. un ataque exitoso de Ransomware, pérdida de una laptop o filtración de datos personales).

2.2. Áreas de Cobertura

- **Incidentes Lógicos:** Virus, denegación de servicios, accesos no autorizados, robo de contraseñas o borrado accidental de bases de datos.
- **Incidentes Físicos:** Robo de equipo de cómputo, acceso no autorizado a oficinas restringidas o daños a la infraestructura por siniestros.
- **Incidentes de Datos:** Fuga de información sensible o incumplimiento en el tratamiento de datos personales de la ciudadanía.

3. Políticas de Gestión de Incidentes

3.1. Cultura de Reporte Obligatorio

Todo colaborador, sin importar su rango o modalidad de contratación, tiene la obligación de reportar cualquier anomalía, evento sospechoso o incidente confirmado de seguridad de la información.

- **Prohibición de Ocultamiento:** Queda estrictamente prohibido intentar resolver incidentes técnicos por cuenta propia o de manera informal sin dejar registro. Ocultar un incidente que ponga en riesgo la información institucional será motivo de revisión administrativa.
- **Mecanismo de Reporte:** El reporte inicial debe formalizarse mediante el **Formato de Registro de Incidentes**, capturando la mayor cantidad de evidencia posible (capturas de pantalla, fotos, descripción de síntomas) en el momento de la detección.

3.2. Clasificación Estandarizada mediante Matriz

Para garantizar una respuesta proporcional al daño, todo evento reportado debe ser evaluado conforme a la **Matriz de Clasificación de Incidentes**.

- **Criterios de Evaluación:** La clasificación se basará en el cruce de **Impacto** (afectación a la confidencialidad, integridad o disponibilidad) y **Urgencia** (tiempo máximo aceptable antes de que el daño sea irreversible).
- **Niveles de Prioridad:** Los incidentes se categorizarán en: **Bajo, Medio, Alto y Crítico**. Esta clasificación dictará los tiempos de respuesta y el nivel de autoridad que debe ser notificado (desde un técnico de soporte hasta el Titular del Ayuntamiento en casos de desastre).

3.3. Equipo de Respuesta a Incidentes (CSIRT-Morelia)

Se establece la creación del equipo de respuesta, integrado por personal de la Dirección de TI, con apoyo de los Enlaces de Capital Humano y el área Jurídica cuando el incidente así lo requiera.

- **Autoridad Operativa:** Durante la gestión de un incidente Crítico o Alto, el equipo de respuesta tiene la autoridad para suspender servicios digitales, bloquear accesos o desconectar equipos de la red de manera preventiva sin previo aviso, con el fin de contener la amenaza.

3.4. Registro y Trazabilidad en Bitácora

Todo incidente, desde su detección hasta su cierre, debe ser documentado en la **Matriz de Bitácora de Incidentes**.

- **Consistencia de Datos:** La bitácora deberá contener las marcas de tiempo (timeline), las acciones de contención realizadas, el personal involucrado y la resolución técnica final.
- **Inmutabilidad del Registro:** Una vez que un incidente se marca como "Cerrado" en la bitácora, el registro no podrá ser modificado, asegurando que la evidencia sea válida para auditorías de la ISO 27001 o procesos legales.

3.5. Institucionalización de las Lecciones Aprendidas

El Ayuntamiento no solo busca corregir fallas, sino evitar su recurrencia. Por ello:

- **Análisis:** Para todo incidente clasificado como Medio, Alto o Crítico, es obligatorio completar la sección de **Lecciones Aprendidas** dentro de la Matriz de Bitácora.
- **Actualización de Controles:** Si el análisis revela que un control actual falló o no existe, la Dirección de TI debe proponer el ajuste a las políticas o la adquisición de nueva tecnología en un plazo no mayor a 30 días tras el cierre del incidente.

3.6. Preservación de Evidencia y Cadena de Custodia

En incidentes que involucren posibles delitos (robo de equipo, sabotaje o fuga de información), el personal de TI debe priorizar la preservación de la evidencia digital.

- **Integridad Forense:** No se debe manipular el equipo afectado más allá de lo necesario para su aislamiento.
- **Coordinación Jurídica:** El reporte generado en el **Formato de Registro de Incidentes** servirá como base para reportar cualquier incidente detectado.

4. Procedimientos

4.1. Detección y Notificación Inicial

El procedimiento inicia en el momento en que un colaborador, sistema de monitoreo o tercero identifica un evento sospechoso o una falla de seguridad. El detector debe proceder

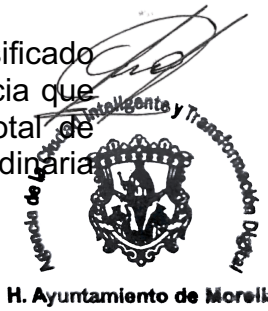
de inmediato con el llenado del **Formato de Registro de Incidentes**, tratándose de equipos de cómputo con apoyo del personal de Tecnologías de su Dependencia o Entidad, cuando se cuente con él, de lo contrario deberá hacerlo del conocimiento de su inmediato superior, quien reportará a la Agencia de la Ciudad Inteligente y Transformación Digital del Ayuntamiento de Morelia de lo sucedido, capturando de forma clara: qué está sucediendo, en qué equipo o sistema, y la hora exacta del hallazgo.

Una vez completado el registro, este debe ser enviado por el canal oficial (correo institucional de soporte o plataforma de tickets) a la Dirección de TI. El personal que reporta tiene prohibido realizar acciones de "limpieza" o reinicio por cuenta propia para evitar la pérdida de evidencia o la propagación accidental de una amenaza.

4.2. Triage y Clasificación mediante Matriz

Al recibir el reporte, el equipo de respuesta (CSIRT) aplica la **Matriz de Clasificación de Incidentes**. En este punto, se cruza el impacto (cuántas dependencias o ciudadanos se ven afectados) con la urgencia (qué tan rápido se degrada el servicio).

El resultado de este cruce dictará la prioridad de atención. Si el incidente es clasificado como **Crítico** (ej. Ransomware en Tesorería), se dispara el protocolo de emergencia que incluye la notificación inmediata al Titular de la dependencia y la asignación total de recursos técnicos para su resolución. Si es **Bajo**, se integra a la cola de atención ordinaria, pero sin omitir su registro formal.



4.3. Contención, Investigación y Erradicación

Con la prioridad establecida, se ejecutan las maniobras de contención para evitar que el incidente crezca. Esto puede incluir el aislamiento de redes, bloqueo de puertos en el Firewall o la suspensión temporal de cuentas de usuario comprometidas.

Simultáneamente, se inicia la investigación técnica para identificar el vector de ataque (cómo entraron) y el alcance del daño. Una vez contenido el incidente, se procede con la erradicación de la causa raíz, eliminando archivos maliciosos, restaurando configuraciones seguras o aplicando parches de emergencia que fueron omitidos. Todas estas acciones técnicas deben ser anotadas cronológicamente para su posterior vaciado en la bitácora.

4.4. Recuperación y Restablecimiento del Servicio

Una vez que el entorno es declarado seguro por la Dirección de TI, se inicia el restablecimiento de los servicios o sistemas afectados. Este proceso se realiza de forma gradual, monitoreando el comportamiento de la red para asegurar que la amenaza no persista de forma latente. En caso de pérdida de datos, se ejecuta el procedimiento de **Gestión de Copias de Seguridad** para recuperar la información hasta el último punto de respaldo válido (RPO), validando siempre la integridad de los datos antes de permitir el acceso a los usuarios finales.

4.5. Cierre de Incidente y Registro en Bitácora

Tras confirmar la normalidad operativa, el incidente se considera técnicamente resuelto, pero el proceso administrativo continúa. El líder del equipo de respuesta debe trasladar toda la información del evento a la **Matriz de Bitácora de Incidentes**.

En esta matriz se consolidará el historial completo: desde quién reportó originalmente hasta qué medidas técnicas se tomaron para la solución definitiva. El registro en la bitácora es el requisito indispensable para dar por cerrado oficialmente el caso ante cualquier auditoría del SGSI.

4.6. Análisis Post-Incidente y Lecciones Aprendidas

Dentro de las 72 horas posteriores al cierre, se realiza la sesión de "Lecciones Aprendidas", cuyos resultados se integran en la sección correspondiente de la **Matriz de Bitácora**. El equipo debe analizar qué control falló, por qué la detección no fue inmediata y qué se puede mejorar para evitar la recurrencia.

Si el análisis arroja la necesidad de capacitar al personal o adquirir nueva tecnología, se genera una recomendación formal que se anexa al plan de mejora del Ayuntamiento. Este paso cierra el ciclo de la **ISO 27001**, convirtiendo un momento de crisis en una oportunidad de fortalecimiento institucional.

5. Definiciones

- **CSIRT (Computer Security Incident Response Team):** Equipo multidisciplinario responsable de recibir, revisar y responder a reportes de incidentes de seguridad.

- **Evento de Seguridad:** Cualquier ocurrencia identificada en un sistema que pueda indicar un fallo en la política de seguridad o la falla de un control.
- **Incidente de Seguridad:** Uno o más eventos de seguridad no deseados que tienen una probabilidad significativa de comprometer las operaciones del Ayuntamiento.
- **Lecciones Aprendidas:** El conocimiento obtenido tras el análisis de un incidente, utilizado para mejorar los controles y evitar que el evento se repita.
- **Triage:** El proceso de categorización y priorización de incidentes basado en su urgencia e impacto.
- **Análisis de Causa Raíz (RCA):** Metodología para identificar el factor fundamental que causó el incidente, en lugar de solo tratar los síntomas.

6. Formatos

Para la correcta ejecución de esta política, es obligatorio el uso y custodia de los siguientes tres instrumentos:

1. **Formato de Registro de Incidentes (F-GI-01):** El documento de entrada donde el usuario o técnico describe el hallazgo inicial.
2. **Matriz de Clasificación de Incidentes (M-GI-01):** Herramienta de decisión técnica que cruza **Impacto vs. Urgencia** para determinar la prioridad (Baja, Media, Alta, Crítica).
3. **Matriz de Bitácora de Incidentes y Lecciones Aprendidas (M-GI-02):** El registro maestro de seguimiento histórico que incluye el análisis de causa raíz y las acciones de mejora post-incidente.

7. Relación Normativa (ISO 27001:2022)

Este documento es el pilar para el cumplimiento de la cláusula de "Gestión de Incidentes" en la nueva versión de la norma:

Control Anexo A	Título del Control	Justificación del Cumplimiento
5.24	**Planeación y preparación**	Se cumple mediante la creación del equipo de respuesta y la definición de las políticas de reporte.
5.25	**Evaluación y decisión**	Se materializa con el uso de la **Matriz de Clasificación** para realizar el triage de eventos.

Control Anexo A	Título del Control	Justificación del Cumplimiento
5.26	**Respuesta a incidentes**	Establecido en los procedimientos de contención, erradicación y recuperación del Punto 4.
5.27	**Aprendizaje de incidentes**	Se garantiza mediante la sección obligatoria de **Lecciones Aprendidas** en la bitácora.
5.28	**Recopilación de evidencia**	Asegurado por el **Formato de Registro** y el resguardo de logs para fines legales o administrativos.