Tabla de contenido

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

1. Propósito

El presente documento tiene como objetivo establecer los lineamientos para la generación, protección, revisión y conservación de los registros de actividad (**logs**) y bitácoras del H. Ayuntamiento de Morelia. Se busca garantizar la trazabilidad total de las acciones realizadas en los sistemas institucionales, permitiendo la detección temprana de anomalías, la reconstrucción de eventos tras un incidente y el cumplimiento de las obligaciones legales en materia de auditoría.

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

- **Visibilidad y Detección Temprana:** Implementar un esquema de monitoreo continuo que permita identificar comportamientos inusuales, intentos de acceso no autorizados o fallos de sistema antes de que afecten la operación ciudadana.
- **Gestión Estructurada de Crisis:** Asegurar que cualquier anomalía sea capturada y categorizada mediante el **Formato de Clasificación de Eventos e Incidentes**, garantizando que los recursos de TI se enfoquen en los riesgos de mayor impacto y prioridad.
- **Evidencia y Trazabilidad:** Mantener un registro histórico inalterable a través de la **Bitácora de Accesos Físicos y Digitales**, permitiendo saber con precisión quién, cuándo y desde dónde se accedió a áreas restringidas (como el SITE) o a bases de datos sensibles.
- **Aseguramiento de la Continuidad:** Verificar la correcta ejecución de las tareas preventivas mediante la **Bitácora de Mantenimiento y Respaldo**, asegurando que los servidores operen bajo configuraciones seguras (Hardening) y que la información cuente con respaldos íntegros.
- **Análisis y Mejora Continua:** Institucionalizar la revisión periódica de la actividad del sistema mediante el **Informe Técnico de Revisión de Registros**, transformando los datos crudos de los logs en inteligencia operativa para la toma de decisiones.
- **Respuesta y Cierre de Brechas:** Documentar de forma exhaustiva la resolución de fallas mediante el **Formato de Registro de Incidentes**, asegurando que cada evento sea analizado para evitar su recurrencia y cumplir con los protocolos de transparencia.

2. Alcance

Esta política es de **cumplimiento obligatorio** para todo el personal de la Dirección de TI, personal de seguridad física, proveedores externos con acceso a sistemas y cualquier usuario con privilegios administrativos. El alcance se extiende a los siguientes niveles:

2.1. Alcance sobre Infraestructura y Sistemas (Registros Digitales)

Aplica a la generación y custodia de logs en:

- **Dispositivos de Red:** Firewalls, Switches administrables, Routers y Access Points.
- **Servidores y Almacenamiento:** Sistemas operativos (Windows Server, Linux), bases de datos (SQL, Oracle) y servicios en la nube (Azure/AWS).

- **Aplicaciones Críticas:** Portales de trámites, sistemas de recaudación, nómina y plataformas de atención ciudadana.
- **Seguridad Perimetral:** Bitácoras de acceso VPN y sistemas de detección de intrusos (IDS/IPS).

2.2. Alcance sobre el Entorno Físico

Rige sobre el control de acceso a áreas restringidas:

- **Centros de Datos (SITE):** Registro de entrada y salida de personal técnico y proveedores.
- **Áreas de Resguardo de Activos:** Almacenes de equipo de cómputo y archivos físicos sensibles.
- **Sistemas de Videovigilancia:** Monitoreo y registro de eventos capturados por cámaras de seguridad institucional.

2.3. Alcance sobre la Gestión de Eventos e Incidentes

Aplica a toda anomalía detectada que pueda poner en riesgo la triada de la información (**Confidencialidad, Integridad y Disponibilidad**):

- **Eventos de Seguridad:** Intentos de login fallidos, escaneos de puertos o cambios no autorizados en privilegios.
- **Eventos de Disponibilidad:** Caídas de servicios, saturación de discos o fallas en el suministro eléctrico detectadas mediante la **Bitácora de Mantenimiento y Respaldo**.
- **Errores Operativos:** Fallos en la ejecución de procesos automáticos o tareas de respaldo.

2.4. Alcance sobre la Documentación y Auditoría

Cubre el ciclo de vida de la evidencia documental:

- **Análisis Mensual:** Generación obligatoria del **Informe Técnico de Revisión de Registros**.
- **Trazabilidad Humana:** Uso de la **Bitácora de Accesos Físicos y Digitales** para correlacionar acciones del sistema con usuarios específicos.
- **Histórico de Incidentes:** Mantenimiento del **Formato de Registro de Incidentes** para auditorías externas de la ISO 27001.

3. Políticas de Gestión de Bitácoras, Registros y Monitoreo

3.1. Generación y Sincronización de Tiempo

Para garantizar la validez legal y técnica de los registros:

- **Sincronización de Relojes:** Todos los sistemas del Ayuntamiento (servidores, equipos de red, bases de datos y cámaras) deben sincronizar su hora con una fuente de tiempo única y confiable. Se utilizará preferentemente el **Controlador de Dominio (Directorio Activo)** para clientes internos, y protocolos **NTP (Network Time Protocol)** apuntando a fuentes oficiales para equipos perimetrales.
- **Estándar Horario:** Se debe utilizar el huso horario oficial de la región (Tiempo del Centro de México) y asegurar que el cambio de horario de verano/invierno (si aplica) sea gestionado automáticamente para evitar saltos en las bitácoras.

3.2. Registro de Eventos y Logs

- **Configuración de Logs:** Los sistemas deben registrar, como mínimo: intentos de inicio de sesión (exitosos y fallidos), creación/modificación de usuarios, acceso a datos sensibles y cambios en configuraciones de sistema; almacenando evento y marca de tiempo hasta nivel de segundos.
- **Integridad de los Registros:** Las bitácoras digitales deben protegerse contra modificaciones no autorizadas. El acceso a los logs debe estar restringido a personal de auditoría o seguridad, impidiendo que el propio administrador del sistema pueda borrar sus huellas.

3.3. Clasificación y Priorización de Incidentes

- **Categorización Obligatoria:** Toda anomalía detectada debe ser procesada mediante el **Formato de Clasificación de Eventos e Incidentes**, asignando un nivel de criticidad (Bajo, Medio, Alto, Crítico) basado en el impacto a la ciudadanía y la confidencialidad de los datos.
- **Escalamiento:** Los incidentes clasificados como "Altos" o "Críticos" deben notificarse de inmediato a la Dirección de TI y ser documentados formalmente en el **Formato de Registro de Incidentes**.

3.4. Control de Acceso Físico y Digital

- **Registro de Movimientos:** Cualquier entrada al SITE o acceso a cuentas con privilegios administrativos (Root/Admin) debe quedar asentado en la **Bitácora de Accesos Físicos y Digitales**.
- **Supervisión de Terceros:** El acceso de proveedores externos debe ser registrado y, en lo posible, monitoreado en tiempo real para asegurar que sus acciones coincidan con lo solicitado en su orden de servicio.

3.5. Mantenimiento, Hardening y Respaldos

- **Estado de Salud del Servidor:** Semanalmente se debe verificar que los servidores mantengan su configuración de seguridad (Hardening) y que los backups se hayan ejecutado sin errores, documentando esto en la **Bitácora de Mantenimiento y Respaldo**.
- **Pruebas de Restauración:** El registro de mantenimiento debe incluir evidencias de que los respaldos son funcionales (pruebas de restauración exitosas).

3.6. Revisión Mensual y Retención

- **Análisis de Tendencias:** El Oficial de Seguridad o el responsable de TI debe realizar una revisión analítica de los logs mensualmente, consolidando los hallazgos en el **Informe Técnico de Revisión de Registros**.
- **Periodo de Retención:** Los registros de auditoría y bitácoras deben conservarse por un periodo mínimo de **12 meses** (o según marque la ley de transparencia local) para permitir investigaciones retrospectivas.

4. Procedimientos

4.1. Configuración de la Línea Base de Monitoreo

Antes de empezar a registrar, se debe asegurar que la fuente de datos sea íntegra:

1. **Sincronización de Tiempo:** El administrador de red verificará que el servidor principal de **Directorio Activo**esté apuntando a un servidor NTP externo confiable (ej. pool.ntp.org o el del CENAM). Todos los dispositivos (firewalls, bases de datos y cámaras) deberán configurarse para replicar la hora de este controlador de dominio.

2. **Activación de Niveles de Log:** Se configurará el nivel de registro en "Advertencia" e "Error" para eventos de sistema, y "Auditoría de éxito y falla" para eventos de acceso a datos y cambios de privilegios.

4.2. Registro y Control de Accesos (Físico y Digital)

Este procedimiento asegura la trazabilidad de quién entra a la infraestructura:

1. **Control de Áreas Seguras:** Todo personal que ingrese al SITE debe registrarse en la **Bitácora de Accesos Físicos y Digitales**, anotando nombre, dependencia/empresa, motivo de entrada, hora de ingreso y hora de salida.
2. **Accesos Administrativos:** Cada vez que un técnico utilice una cuenta con privilegios elevados (ej. Administrator, root o sa), deberá quedar asentado en la bitácora digital el número de ticket de soporte o cambio que justifica dicha sesión.

4.3. Rutina de Mantenimiento y Verificación de Hardening

Para garantizar que el servidor sigue siendo una "fortaleza":

1. **Revisión de Configuración Segura:** Semanalmente, se cotejará que los servidores no hayan sufrido cambios en sus parámetros de seguridad (puertos abiertos innecesarios, servicios desactivados).
2. **Validación de Respaldos:** Se verificará el log de éxito de las tareas de backup nocturnas.
3. **Documentación:** Ambos procesos se registrarán en la **Bitácora de Mantenimiento y Respaldo**, firmando la conformidad del estado actual del servidor.

4.4. Clasificación y Tratamiento de Incidentes

Cuando se detecta una anomalía (ya sea por monitoreo automático o reporte humano):

1. **Triage de Seguridad:** Se utiliza el **Formato de Clasificación de Eventos e Incidentes** para determinar la severidad. Si el incidente afecta a un sistema ciudadano (ej. Pagos en línea), se clasifica automáticamente como "Crítico".
2. **Documentación del Hallazgo:** Se abre el **Formato de Registro de Incidentes**, capturando la evidencia (capturas de pantalla, fragmentos de log) y describiendo el impacto inicial.

3. **Resolución y Cierre:** Una vez contenido el incidente, se documentan las acciones de remediación y se cierra el formato con una sección de "Lecciones Aprendidas" para evitar que el fallo se repita.

4.5. Análisis Mensual y Generación de Reportes

Este paso es fundamental para la rendición de cuentas ante auditorías ISO:

1. **Análisis de Logs:** El Oficial de Seguridad o el responsable de TI realizará una extracción de los eventos más relevantes del mes (intentos de intrusión bloqueados, fallas de hardware, accesos fuera de horario).
2. **Emisión del Informe:** Se genera el **Informe Técnico de Revisión de Registros**, donde se resumen las métricas del mes, los incidentes resueltos y el estado de salud de la infraestructura. Este reporte se entrega a la Dirección de TI para su validación.

5. Definiciones

- **Log (Registro de Actividad):** Archivo generado automáticamente por un sistema que registra eventos, errores y transacciones realizadas por usuarios o procesos.
- **Hardening (Endurecimiento):** Proceso de asegurar un sistema mediante la reducción de su superficie de vulnerabilidad, eliminando funciones, puertos y servicios innecesarios.
- **NTP (Network Time Protocol):** Protocolo de red destinado a la sincronización de los relojes de los sistemas informáticos a través de la red.
- **Evento de Seguridad:** Una ocurrencia identificada en un sistema, servicio o red que indica una posible brecha de la política de seguridad o falla de controles.
- **Incidente de Seguridad:** Un evento o serie de eventos de seguridad no deseados o inesperados que tienen una probabilidad significativa de comprometer las operaciones del Ayuntamiento.
- **Trazabilidad:** La capacidad de recrear la historia, el uso o la localización de una entidad (un dato o un acceso) mediante registros documentados.
- **SIEM (Security Information and Event Management):** (Opcional) Herramienta tecnológica que centraliza y analiza los logs de múltiples fuentes en tiempo real.

6. Formatos

Para que el monitoreo sea auditable, la Dirección de TI debe operar bajo los siguientes registros oficiales:

1. **F-MON-01: Formato de Registro de Incidentes**
   - *Uso:* Documentar el ciclo de vida de una falla o ataque, desde su detección hasta su cierre.
2. **F-MON-02: Bitácora de Mantenimiento y Respaldo**
   - *Uso:* Registro semanal de tareas de salud del servidor, incluyendo el cumplimiento del hardening y éxito de backups.
3. **F-MON-03: Formato de Clasificación de Eventos e Incidentes**
   - *Uso:* Herramienta de "Triage" para asignar prioridad y nivel de impacto a lo detectado.
4. **F-MON-04: Informe Técnico de Revisión de Registros**
   - *Uso:* El reporte ejecutivo mensual que resume el análisis de logs y el estado de seguridad institucional.
5. **F-MON-05: Bitácora de Accesos Físicos y Digitales**
   - *Uso:* Control nominal de quién entra al SITE y quién utiliza cuentas administrativas críticas.

H. Ayuntamiento de Morelia

7. Relación Normativa (ISO 27001:2022)

Este documento es el sustento técnico para los siguientes controles internacionales:

Control	Título	Justificación del Cumplimiento
8.15	**Registro de eventos**	Establece la obligatoriedad de generar logs de actividad y protegerlos contra alteraciones.
8.16	**Monitoreo de actividades**	Se cumple mediante la revisión sistemática de bitácoras y la generación del **Informe Técnico mensual**.
8.17	**Sincronización de relojes**	Garantiza la coherencia temporal de todos los registros mediante el uso del **Directorio Activo** y NTP.
5.24	**Gestión de incidentes de seguridad**	Define el flujo de captura, clasificación y respuesta ante anomalías mediante los formatos correspondientes.
8.11	**Gestión de la configuración**	Se vincula con la bitácora de mantenimiento para asegurar que el hardening se mantenga en el tiempo.