Unidad de Transparencia
San Ciro de Acosta, S.L.P

SAN CIRO DE ACOSTA

SAN LUIS POTOSI

H. AYUNTAMIENTO 2024 I 2027

DOCUMENTO DE SEGURIDAD

UNIDAD DE TRANSPARENCIA

ELABORADO POR:

C. OMAR ARTEAGA FLORES

OFICIAL DE DATOS PERSONALES

ÍNDICE

I. DISPOSICIONES GENERALES

DATOS GENERALES

- **Sujeto Obligado:** H. Ayuntamiento de San Ciro de Acosta.
- **Domicilio:** Palacio Municipal S/N, Col. Centro, C.P. 79680, San Ciro de Acosta, S.L.P.
- **Responsable de Elaboración:** Unidad de Transparencia
- **Marco Jurídico:** Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de San Luis Potosí

I.1 OBJETIVO

El presente Documento de Seguridad tiene por objeto establecer las medidas administrativas, técnicas y físicas necesarias para la protección de los datos personales en posesión del Ayuntamiento de San Ciro de Acosta, en cumplimiento con la Ley de Protección de Datos Personales del Estado de San Luis Potosí.

I.2 ÁMBITO DE APLICACIÓN

El presente documento es de observancia obligatoria para todas las áreas administrativas, servidores públicos y cualquier persona que intervenga en el tratamiento de datos personales.

I.3 FUNDAMENTO JURÍDICO

Este documento se sustenta en:

Constitución Política de los Estados Unidos Mexicanos, que a la letra dicen:

Artículo 6o. La manifestación de las ideas no será objeto de ninguna inquisición judicial o administrativa, sino en el caso de que ataque a la moral, la vida privada o los derechos de terceros, provoque algún delito, o perturbe el orden público; el derecho de réplica será ejercido en los términos dispuestos por la ley. El derecho a la información será garantizado por el Estado. Párrafo reformado

Toda persona tiene derecho al libre acceso a información plural y oportuna, así como a buscar, recibir y difundir información e ideas de toda índole por cualquier medio de expresión. Párrafo adicionado

El Estado garantizará el derecho de acceso a las tecnologías de la información y comunicación, así como a los servicios de radiodifusión y telecomunicaciones, incluido el de banda ancha e Internet. Para tales efectos, el Ejecutivo Federal a través de la dependencia encargada de elaborar y conducir las políticas de telecomunicaciones y radiodifusión, establecerá condiciones de competencia efectiva en la prestación de dichos servicios.

Articulo16. Párrafo Segundo:

Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros.

Ley de Protección de Datos Personales del Estado de San Luis Potosí

Artículo 3 Fracción XIII:

XIII. Documento de seguridad: instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee;

Ley de Transparencia y Acceso a la Información Pública del Estado de San Luis Potosí

II. DEFINICIONES

Para efectos del presente documento se entenderá por:

Datos personales: Cualquier información concerniente a una persona física identificada o identificable.

Datos personales sensibles: Aquellos que afectan la esfera más íntima del titular.

Tratamiento: Cualquier operación o conjunto de operaciones realizadas sobre datos personales.

Responsable: Oficial de Datos Personales: Omar Arteaga Flores

III. PRINCIPIOS RECTORES

El tratamiento de datos personales deberá regirse por los siguientes principios:

- Licitud
- Finalidad
- Lealtad
- Consentimiento
- Calidad
- Proporcionalidad
- Información
- Responsabilidad

IV. ESTRUCTURA ORGÁNICA

IV.1 RESPONSABLE

El Ayuntamiento de San Ciro de Acosta es el responsable del tratamiento de datos personales.

IV.2 UNIDAD DE TRANSPARENCIA

Será la encargada de supervisar el cumplimiento normativo y atender solicitudes de derechos ARCO.

IV.3 ENCARGADOS

Directores y jefes de departamento encargados de las áreas administrativas que traten datos personales serán consideradas encargadas.

V. INVENTARIO DE DATOS PERSONALES

El Ayuntamiento gestiona diversos sistemas de tratamiento. Para cada uno de ellos, se mantiene un registro detallado que incluye:

Identificación del Sistema: (Ejemplo: Sistema de Trámites de Registro Civil, Padrón de Catastro, Expedientes de Seguridad Pública).

Finalidades: El objetivo legítimo para el cual se recaban los datos.

Categorías de Datos: Identificación: Nombre, domicilio, CURP, RFC, firma.

Sensibles: Huellas dactilares, estado de salud o pertenencia a grupos vulnerables (principalmente en DIF y Seguridad).

Ciclo de Vida: Se documenta el método de obtención, el soporte (físico en archivos municipales o digital en servidores locales) y los plazos de conservación antes de su transferencia al Archivo Histórico o su destrucción segura.

El Ayuntamiento deberá mantener un inventario actualizado de:

Bases de datos

Sistemas de información

Archivos físicos y digitales

Finalidades del tratamiento

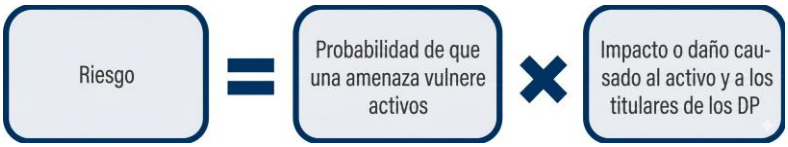
Este inventario debe ser completado por cada área (Tesorería, Registro Civil, Seguridad Pública, etc.)

CAMPO DEL INVENTARIO	DESCRIPCIÓN DEL CONTENIDO
Nombre del Tratamiento	Ejemplo: "Sistema de Registro Civil" o "Padrón de Proveedores".
Finalidad	El objetivo legal (ej. expedición de actas, pagos de servicios).
Categorías de Datos	Identificación (nombre, CURP), contacto (teléfono), sensibles (biométricos, salud).
Soporte	Físico (archiveros) o Electrónico (servidores/nube).
Transferencias	Indicar disposición final de los datos
Plazo de Conservación	Conforme al Catálogo de Disposición Documental del Ayuntamiento.

VI. ANÁLISIS DE RIESGOS

¿Qué es un riesgo?
De acuerdo con la Guía para implementar un SGSDP Junio 2015, el riesgo es la combinación de la probabilidad de un evento y su consecuencia desfavorable. Otra definición, retomada de la **Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (MAGERIT),** establece que un riesgo es la estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos, causando daños o perjuicios a la Organización6.

En otras palabras, es posible definir un riesgo a partir de la interacción de amenazas que atacan una o diversas vulnerabilidades de un activo o grupo de activos en perjuicio de la organización; en este caso de la entidad. Por ello, cuando un riesgo se materializa ocurre un incidente de seguridad, el cual se traduce en una violación a las medidas de seguridad.



¿Qué es un riesgo inherente?

Según la definición técnica, el riesgo inherente es la valoración del grado de exposición de un activo a una amenaza que pueda explotar su vulnerabilidad, sin considerar ninguna medida de seguridad implementada.

En el caso que nos ocupa es decir, tratándose de los datos personales como activo adoptaremos como definición de riesgo inherente aquellos factores que le dan un valor significativo como para que cualquier persona no autorizada pudiera beneficiarse de ellos, causando un mayor impacto en los titulares y/o en sus derechos y libertades. El riesgo inherente en los sistemas de tratamiento de datos personales puede incrementar cuando se manejan grandes volúmenes de información personal, cuando se relacionan distintos tipos de datos o se combinan bases de datos de diferentes fuentes (cruces de información), o bien cuando los datos que se tratan son sensibles.

El nivel de riesgo en los sistemas de tratamiento de datos personales puede disminuirse con mecanismos como: Disociación: Se aíslan los datos de modo que por sí no aporten información valiosa de una persona titular o esta no pueda ser identificable. Así, el valor de la base de datos para una persona no autorizada se ve disminuido.

Separación: Se separan los activos de información grandes en otros más pequeños. Por ejemplo, una base de datos de clientes en dos bases de datos: clientes corporativos y personas físicas. Entre mayor cantidad de información tiene un activo, este resulta más atractivo para una persona no autorizada Es importante identificar este tipo de riesgo para ayudar a cuantificar el riesgo a partir del nivel de interés que puede generar en un atacante.

El Ayuntamiento deberá identificar, analizar y mitigar riesgos asociados al tratamiento de datos personales mediante:

- Identificación de activos
- Identificación de amenazas
- Evaluación de vulnerabilidades
- Determinación del nivel de riesgo

VII. MEDIDAS DE SEGURIDAD

VII.1 ADMINISTRATIVAS (ABC)

A. Políticas Internas de Protección de Datos

Estas directrices rigen el comportamiento diario de los servidores públicos en el manejo de la información:

- **Manual de Procedimientos de Privacidad:** Establecer un protocolo escrito que defina cómo se recolectan, almacenan y eliminan los datos personales en cada dirección (Tesorería, Registro Civil, Seguridad Pública, etc.).

- **Gestión de Inventarios:** Obligación de mantener actualizado el inventario de datos personales, identificando quién es el titular de cada base de datos dentro del ayuntamiento.

- **Procedimiento de Borrado Seguro:** Implementar una política para la eliminación definitiva de archivos digitales y la trituración de documentos físicos una vez agotado su Plazo de Conservación.

B. Capacitación del Personal

El personal debe ser consciente de que la protección de datos es una obligación legal y no opcional:

- **Programa de Inducción:** Todo nuevo empleado del Ayuntamiento de San Ciro de Acosta deberá recibir una sesión informativa sobre sus responsabilidades bajo la Ley de Protección de Datos Personales de San Luis Potosí.

- **Capacitación Especializada:** Talleres técnicos para las áreas que manejan datos sensibles (DIF, Salud, Catastro) sobre cómo identificar riesgos y evitar fugas de información.

- **Evaluación de Conocimientos:** Realizar diagnósticos periódicos para asegurar que los enlaces de cada área comprenden el ejercicio de los Derechos ARCO.

C. Confidencialidad

Garantizar que la información no sea divulgada a terceros sin fundamento legal:

- **Cartas de Confidencialidad:** Firma obligatoria de compromisos de confidencialidad por parte de todos los funcionarios, empleados y prestadores de servicios externos.
- **Gestión de Terceros:** Antes de transferir datos a otras instituciones o proveedores, se debe verificar que estos cuenten con medidas de seguridad equivalentes a las del Ayuntamiento.

Control Administrativo	Frecuencia / Aplicación	Responsable
Revisión de Políticas	Anual	Unidad de Transparencia
Capacitación	Semestral	Recursos Humanos / UT
Firma de Confidencialidad	Al ingreso del personal	Contraloría Interna

VII.2 TÉCNICAS (ABC)

Estas medidas comprenden el conjunto de acciones y herramientas para proteger el entorno digital donde residen los datos personales.

A. Control de Accesos

El acceso a la información debe ser restrictivo y basado en la función del servidor público.

- **Perfiles de Usuario:** Implementar el principio de "mínimo privilegio". Cada empleado tendrá acceso únicamente a los módulos de software o carpetas compartidas estrictamente necesarios para su labor (ej. personal de Limpieza no accede a Nómina), bajo un criterio de que cada quien es responsable del resguardo de la información que se encuentra en su equipo de trabajo y de su acceso propio o compartido entre sus auxiliares administrativos para el manejo de los datos.
- **Autenticación Individual:** Queda estrictamente prohibido el uso de cuentas compartidas o genéricas. Cada servidor público deberá ingresar con un identificador único para garantizar la trazabilidad, evitar con esto de que puedan utilizar algún perfil ajeno al propio para manipular o sustraer información que no esté autorizado por el Jefe de Área.
- **Bloqueo de Sesión Inactiva:** Configuración automática de bloqueo de pantalla tras 5 minutos de inactividad para evitar accesos no autorizados en equipos desatendidos, con esto minimizar el riesgo de que puedan sustraer información sin que el Jefe de Área se encuentre presente en su equipo.

- **Privilegios de Administrador:** El acceso a bases de datos y configuraciones críticas quedará reservado exclusivamente al área de o Sistemas del H. Ayuntamiento de San Ciro de Acosta S.L.P.

B. Uso de Contraseñas Seguras

La primera línea de defensa contra accesos externos e internos no autorizados.

- **Estándar de Complejidad:** Las contraseñas deberán tener una longitud mínima de 10 caracteres, incluyendo mayúsculas, minúsculas, números y caracteres especiales (#, $, %), con el fin de que sea más seguro cada acceso esto también significa que al entregar el cargo tendrán que otorgar la contraseña impuesta al equipo en cuestión

- **Vigencia y Renovación:** Obligatoriedad de cambio de contraseña cada 90 días, impidiendo la reutilización de las últimas tres contraseñas anteriores.

- **Protección de Credenciales:** Prohibición de anotar contraseñas en lugares físicos visibles (post-its, debajo del teclado) o compartirlas a través de medios no cifrados como WhatsApp o correo electrónico.

C. Respaldos de Información

Garantizar la disponibilidad de los datos ante fallos técnicos o ciber ataques contra el H. Ayuntamiento de San Ciro de Acosta, S.L.P.

- **Periodicidad de Backup:** Realización de respaldos automáticos diarios para bases de datos críticas y semanales para archivos administrativos.

- **Almacenamiento Seguro (Regla 3-2-1):**

    - Mantener 3 copias de los datos.
    - En 2 soportes diferentes (Servidor local y Disco duro externo).
    - 1 copia fuera de la ubicación física (Nube cifrada o en una sede alterna del Ayuntamiento).

- **Pruebas de Restauración:** Realizar simulacros trimestrales para verificar que los respaldos funcionan correctamente y que la información puede recuperarse íntegramente.

Medida Técnica	Herramienta / Acción	Responsable
Control de Acceso	Directorio Activo / Permisos NTFS	Sistemas
Contraseñas	Política de grupo en Windows	Sistemas / Usuario
Respaldos	Software de backup cifrado	Sistemas

VII.3 FÍSICAS (ABC)

A. Acceso Restringido a Instalaciones

El objetivo es evitar el acceso de personal no autorizado a las áreas donde se maneja información sensible o confidencial.

- **Control de Ingreso:** Implementar bitácoras de registro para visitantes en oficinas que manejen datos personales. Se requiere identificación oficial para permitir el paso a áreas críticas.
- **Seguridad de Puertas:** Garantizar que las puertas de las oficinas con expedientes cuenten con cerraduras funcionales. El acceso debe estar limitado exclusivamente al personal adscrito a dicha área.
- **Señalética:** Colocación de avisos de "Área Restringida" o "Acceso Exclusivo a Personal Autorizado" en los perímetros del archivo y departamentos estratégicos (Tesorería, Jurídico, etc.).

B. Resguardo de Archivos Físicos

Protección contra el robo, la pérdida o la consulta indebida de documentos en papel.

- **Mobiliario Seguro:** Los expedientes con datos personales deben almacenarse en archiveros con llave. La llave debe estar bajo el resguardo de un responsable designado por el área.
- **Política de "Escritorio Limpio":** Al terminar la jornada laboral o al ausentarse por tiempos prolongados, ningún documento con datos personales debe quedar sobre los escritorios. Todo debe ser guardado en cajones bajo llave.
- **Gestión de Archivos Inactivos:** Traslado periódico de expedientes que ya no están en trámite al Archivo Municipal, asegurando que el traslado cumpla con protocolos de seguridad para evitar extravíos.

C. Protección Contra Siniestros

Prevención de daños accidentales o provocados por agentes externos.

- **Prevención de Incendios:** Instalación y mantenimiento anual de extintores (tipo ABC) en áreas de archivo y cerca de los centros de cómputo. Prohibición estricta de fumar o usar equipos de calefacción no autorizados cerca de documentos.

- **Prevención de Humedad e Inundaciones:** Ubicación de archivos físicos en estanterías elevadas (mínimo 15 cm del suelo) para prevenir daños por inundaciones, fugas de tuberías o filtraciones.
- **Control Ambiental:** Evitar la exposición directa de documentos a la luz solar y mantener niveles adecuados de ventilación para prevenir la degradación de los materiales.

Medida Física	Acción Preventiva	Responsable
Acceso	Registro de visitantes y cierre de puertas	Jefe de Área
Resguardo	Uso de archiveros bajo llave	Servidores Públicos
Siniestros	Revisión de extintores y estanterías	Protección Civil / Archivo

VIII. CONTROL DE ACCESO

Este apartado establece los mecanismos para asegurar que solo las personas autorizadas tengan acceso a los datos personales, ya sea en sistemas digitales o archivos físicos.

VIII.1 Asignación de Usuarios

El proceso de dar de alta a un funcionario en los sistemas debe ser formal y documentado.

- **Cuentas Nominales:** Queda estrictamente prohibido el uso de usuarios genéricos ("usuario1" o "recepción"). Cada cuenta debe estar ligada al nombre del servidor público.
- **Niveles de Privilegio:** La asignación se hará bajo el perfil de "Mínimo Privilegio Necesario". El personal solo tendrá acceso a los módulos indispensables para su cargo.
- **Solicitud Formal:** Todo usuario nuevo debe ser solicitado por el Jefe de Área mediante un oficio o formato interno dirigido al área de Informática/Sistemas.

VIII.2 Bitácoras de Acceso

La bitácora permite saber "quién hizo qué y cuándo".

- **Registros Digitales:** Los sistemas del Ayuntamiento (nómina, registro civil, catastro) deben generar automáticamente un registro que guarde:
    - ID de usuario.
    - Fecha y hora de ingreso/salida.
    - Acción realizada (consulta, modificación o eliminación).

- **Registros Físicos:** Para las áreas de archivo, se utilizará la Bitácora de Control de Acceso a Instalaciones (mencionada en el punto anterior) para registrar el ingreso de personal externo o de otras áreas.

- **Revisión Periódica:** La Unidad de Transparencia o el área de Sistemas revisará aleatoriamente las bitácoras cada mes para detectar intentos de acceso no autorizados.

VIII.3 Revocación de Permisos

Tan importante es dar el acceso como quitarlo a tiempo para evitar "usuarios fantasma".

- **Baja Inmediata por Cese:** En cuanto un servidor público deje de laborar en el Ayuntamiento (renuncia, despido o fin de administración), el Área de Recursos Humanos debe notificar a Sistemas para la cancelación de accesos en un plazo no mayor a 24 horas.

- **Cambio de Funciones:** Si un empleado es transferido de Tesorería a Educación y Cultura, sus permisos anteriores deben ser revocados y asignados los nuevos acordes a su nueva función.

- **Auditoría Anual de Usuarios:** Al menos una vez al año, se realizará un barrido total de las cuentas activas para eliminar aquellas que ya no tengan justificación de uso.

Puesto	Sistema / Archivo	Nivel de Acceso	Tipo de Usuario
Oficinista DIF	Expedientes de Apoyos	Consulta y Registro	Nominal
Tesorería	Base de Datos Predial	Consulta, Edición y Reportes	Nominal
Transparencia	Sistema de Solicitudes	Administrador	Nominal

IX. GESTIÓN DE INCIDENTES

Se considera incidente de seguridad cualquier evento que comprometa la confidencialidad, integridad o disponibilidad de los datos personales (ej. robo de una laptop, pérdida de un USB, hackeo del servidor o extravío de un expediente físico).

1. Detección

El personal del Ayuntamiento debe estar alerta para identificar anomalías.

- **Fuentes de detección:** Reporte directo del empleado, alertas del antivirus, quejas de ciudadanos o detección de accesos inusuales en bitácoras.

- **Clasificación inicial:** Determinar si el incidente es Físico (robo de archivos) o Técnico (virus/hackeo).

2. Notificación

La rapidez es clave para el cumplimiento legal.

- **Interna:** El empleado que detecte el incidente debe informar de inmediato a su Jefe de Área y a la Unidad de Transparencia en un plazo no mayor a 2 horas.
- **Externa:** Si el incidente afecta gravemente los derechos de los titulares, el Ayuntamiento de san Ciro de Acosta, tiene la obligación de notificar a la CEGAIP y, en ciertos casos, a los ciudadanos afectados.

3. Evaluación

Se analiza la magnitud del problema.

- **Alcance:** ¿Cuántas personas se ven afectadas? ¿Qué tipo de datos se perdieron (nombres, domicilios o datos sensibles como salud)?
- **Impacto:** Determinar si el incidente pone en riesgo la identidad, el patrimonio o la seguridad de los titulares de San Ciro de Acosta.

4. Mitigación

Acciones inmediatas para detener el daño.

- **Técnica:** Desconectar equipos de la red, cambiar contraseñas de forma masiva o bloquear cuentas comprometidas.
- **Física:** Levantar denuncia ante el Ministerio Público en caso de robo y dar aviso a la Contraloría Municipal.
- **Recuperación:** Activar los respaldos de información (backups) mencionados en la sección técnica.

5. Registro

Todo incidente debe dejar una huella documental para evitar que se repita.

- **Libro de Incidentes:** Crear un expediente donde se documente: fecha, descripción del evento, acciones tomadas y medidas preventivas adoptadas a futuro.
- **Análisis Post-Mortem:** Reunión de mejora para ajustar las medidas de seguridad y evitar que la vulnerabilidad sea explotada nuevamente.

Fase	Acción Clave	Plazo Sugerido
Detección	Identificar la fuga o pérdida	Inmediato
Notificación	Aviso a la Unidad de Transparencia	< 2 horas
Mitigación	Contener el datos (bloqueo/denuncia)	< 24 horas
Registro	Documentar en el historial	< 48 horas

X. DERECHOS ARCO

El Ayuntamiento de San Ciro de Acosta garantiza a todos los titulares el derecho constitucional de controlar sus datos personales mediante el ejercicio de los derechos **ARCO**.

Definición de los Derechos

- **Acceso:** El ciudadano tiene derecho a solicitar y obtener información sobre qué datos personales suyos están siendo tratados por el ayuntamiento y bajo qué condiciones.
- **Rectificación:** Permite corregir datos que sean inexactos, incompletos o desactualizados (ej. corrección de un apellido en el Registro Civil o domicilio en Catastro).
- **Cancelación:** El titular puede solicitar que se eliminen sus datos de los archivos municipales cuando considere que ya no son necesarios para la finalidad que fueron recabados o el plazo legal de conservación ha vencido.
- **Oposición:** El derecho de impedir el uso de los datos para fines específicos o por causas legítimas propias de su situación personal.

X.2 Procedimiento de Atención

Para asegurar una respuesta legal y oportuna, se establece el siguiente flujo:

1. **Recepción:** La solicitud se recibirá a través de la **Unidad de Transparencia**, ya sea de forma física en las oficinas de la Presidencia Municipal o mediante la **Plataforma Nacional de Transparencia (PNT)**.
2. **Requisitos:** El solicitante debe acreditar su identidad (INE, Pasaporte o Cartilla) para evitar entregas de información a personas no autorizadas.

3. **Plazos Legales:**

    - **Respuesta:** El Ayuntamiento tiene un plazo máximo de **20 días hábiles** para responder sobre la procedencia de la solicitud.

    - **Ejecución:** Si procede, el derecho se hará efectivo en los **15 días hábiles** siguientes a la respuesta.

4. **Gratuidad:** El ejercicio de estos derechos es gratuito. Solo podrán cobrarse los gastos de reproducción (copias simples o certificadas) y envío, conforme a la Ley de Ingresos Municipal vigente.

X.3 Medios de Contacto

Toda solicitud de derechos ARCO en San Ciro de Acosta deberá dirigirse a:

- **Responsable:** Titular de la Unidad de Transparencia.
- **Ubicación:** Planta Alta, Palacio Municipal, San Ciro de Acosta, S.L.P.
- **Correo Electrónico Institucional:** transparenciasanciro@gmail.com

XI. TRANSFERENCIA DE DATOS

Se entiende por transferencia cualquier comunicación de datos personales realizada a una persona distinta del responsable (H. Ayuntamiento) o del encargado (proveedores de servicios).

1. **Transferencias Nacionales**

El Ayuntamiento de San Ciro de Acosta podrá realizar transferencias de datos en los siguientes supuestos:

- **Obligaciones Legales:** Cuando la transferencia esté prevista en una Ley (ej. informes a la Auditoría Superior del Estado, reportes al INEGI o requerimientos judiciales).
- **Interés Público:** Transferencias necesarias para la procuración o administración de justicia (ej. colaboración con la Fiscalía General del Estado).
- **Ejercicio de Facultades:** Entre dependencias del mismo Ayuntamiento, siempre que los datos se utilicen para las finalidades que motivaron su obtención (ej. Tesorería compartiendo datos con Desarrollo Social para validar un apoyo).

2. **Cláusulas de Transferencia y Convenios**

Para asegurar que los datos sigan protegidos fuera del Ayuntamiento:

- **Convenios de Colaboración:** Toda transferencia recurrente con otras instituciones debe estar respaldada por un convenio que estipule las medidas de seguridad que el receptor debe aplicar.

- **Comunicación de Avisos de Privacidad:** El Ayuntamiento debe informar al receptor sobre las finalidades a las que el titular sujetó el tratamiento de sus datos.

- **Responsabilidad Compartida:** El receptor de los datos se convierte en responsable de su tratamiento y debe garantizar niveles de protección equivalentes a los del Ayuntamiento.

3. Excepciones al Consentimiento

Conforme a la Ley, el Ayuntamiento no requerirá el consentimiento del titular para transferir sus datos cuando:

1. Esté prevista en una Ley.
2. Sea necesaria para la prevención o el diagnóstico médico.
3. Sea necesaria por virtud de un contrato celebrado en interés del titular.
4. Sea legalmente exigida para la salvaguarda de un interés público.

XII. AUDITORÍAS

El Ayuntamiento de San Ciro de Acosta establece un sistema de verificación periódica para evaluar la eficacia de las medidas de seguridad y asegurar la mejora continua en la protección de datos personales.

1. Auditorías Internas (Autoevaluación)

La Unidad de Transparencia, en coordinación con el Órgano Interno de Control, realizará revisiones programadas:

- **Periodicidad:** Se llevará a cabo una revisión semestral de los expedientes y sistemas.

- **Alcance:** Verificación de bitácoras de acceso, vigencia de contraseñas, estado físico de los archiveros y existencia de cartas de confidencialidad firmadas por el personal de nuevo ingreso.

- **Muestreo:** Revisión aleatoria en áreas críticas como Registro Civil, Tesorería y DIF Municipal.

2. **Auditorías Externas**

El Ayuntamiento podrá ser sujeto a verificaciones por parte de organismos facultados:

- **Órgano Garante:** Atender las verificaciones que la **CEGAIP** (Comisión Estatal de Garantía de Acceso a la Información Pública) determine realizar para validar el cumplimiento de la Ley estatal.
- **Entes Fiscalizadores:** Facilitar la revisión de procesos de manejo de información durante las auditorías de la Auditoría Superior del Estado **(ASE).**

3. **Informe de Resultados y Plan de Mejora**

El resultado de cada auditoría debe quedar documentado:

- **Hallazgos y Observaciones:** Identificación de brechas de seguridad (un archivero sin llave, equipo sin contraseña o un software sin actualizar).
- **Acciones Correctivas:** Designación de responsables y plazos específicos para solventar las deficiencias encontradas.
- **Seguimiento:** Verificación de que las medidas correctivas se hayan implementado eficazmente antes de la siguiente revisión.

XIII. CAPACITACIÓN

El factor humano es el elemento más relevante en la protección de datos personales. El Ayuntamiento de San Ciro de Acosta implementará un programa permanente de formación para sensibilizar y especializar a los servidores públicos en el manejo responsable de la información.

1. **Programa Anual de Capacitación**

La Unidad de Transparencia, en coordinación con el área de Recursos Humanos, diseñará un calendario anual que incluya:

- **Inducción a Nuevos Ingresos:** Todo personal que se incorpore al Ayuntamiento deberá recibir una sesión informativa obligatoria sobre el Aviso de Privacidad y sus deberes de secrecía antes de manejar datos personales.
- **Actualización Jurídica:** Sesiones sobre reformas a la Ley de Protección de Datos Personales del Estado de San Luis Potosí y criterios emitidos por la CEGAIP.
- **Seguridad Digital:** Talleres prácticos sobre prevención de *phishing*, creación de contraseñas seguras y uso correcto del correo electrónico institucional en conjunto con el área de Sistemas.

2. **Perfiles de Capacitación**

La formación se dividirá según el nivel de responsabilidad:

- **Nivel General:** Sensibilización para todo el personal sobre la importancia de la privacidad y el respeto a los derechos **ARCO.**
- **Nivel Especializado:** Dirigido a áreas con alto manejo de datos sensibles (DIF, Registro Civil, Seguridad Pública, UBR), enfocado en protocolos de resguardo físico y digital.
- **Nivel Directivo:** Capacitación sobre las responsabilidades legales y las posibles sanciones administrativas por el incumplimiento de las medidas de seguridad.

3. **Registro y Constancias**

Para efectos de auditoría y evidencia ante órganos garantes, se mantendrá un expediente de capacitación:

- **Listas de Asistencia:** Registro firmado por cada servidor público que asista a los cursos o talleres.
- **Evaluaciones:** Aplicación de diagnósticos de conocimientos para medir la efectividad de la capacitación.
- **Constancias:** Entrega de reconocimientos que acrediten la participación del personal en programas de protección de datos.

XIV. ACTUALIZACIÓN

El presente Documento de Seguridad es un instrumento dinámico. El Ayuntamiento de San Ciro de Acosta se compromete a revisarlo y actualizarlo periódicamente para garantizar que las medidas de seguridad sigan siendo eficaces frente a nuevas amenazas o cambios institucionales.

XIV.1 Periodicidad de la Revisión

- **Revisión Ordinaria:** El Comité de Transparencia, en conjunto con el área del Órgano Interno de Control, realizará una revisión integral del documento de manera **anual** (preferentemente durante el primer trimestre de cada año).
- **Actualización Extraordinaria:** Se deberá modificar el documento de forma inmediata cuando ocurra cualquiera de los siguientes supuestos:

    1. **Reformas Legales:** Cambios en la Ley de Protección de Datos Personales del Estado de San Luis Potosí o lineamientos de la **CEGAIP**.

2. **Cambios en los Tratamientos:** Cuando se cree un nuevo programa social, sistema de registro o se modifiquen las finalidades de uno existente.

3. **Incidentes de Seguridad:** Si una vulneración de datos revela que las medidas actuales son insuficientes.

4. **Cambios Tecnológicos:** Implementación de nuevo software, servidores o migración de datos a la nube.

XIV.2 Procedimiento de Modificación

1. **Detección de Necesidad:** La Unidad de Transparencia o cualquier Jefe de Área identifica la necesidad de cambio.

2. **Propuesta de Mejora:** Se redacta el ajuste técnico o administrativo correspondiente.

3. **Validación Técnica:** El área de Informática valida que el cambio sea factible y seguro.

4. **Aprobación Oficial:** Las modificaciones deben ser sometidas a votación y aprobadas por el **Comité de Transparencia** del Ayuntamiento.

XV. APROBACIÓN

El presente documento deberá ser aprobado por el Comité de Transparencia del Ayuntamiento de San Ciro de Acosta.