TRANSPARENCIA PARA EL PUEBLO DE CHIAPAS

GOBIERNO DE CHIAPAS 2024 - 2030

HUMANISMO QUE TRANSFORMA

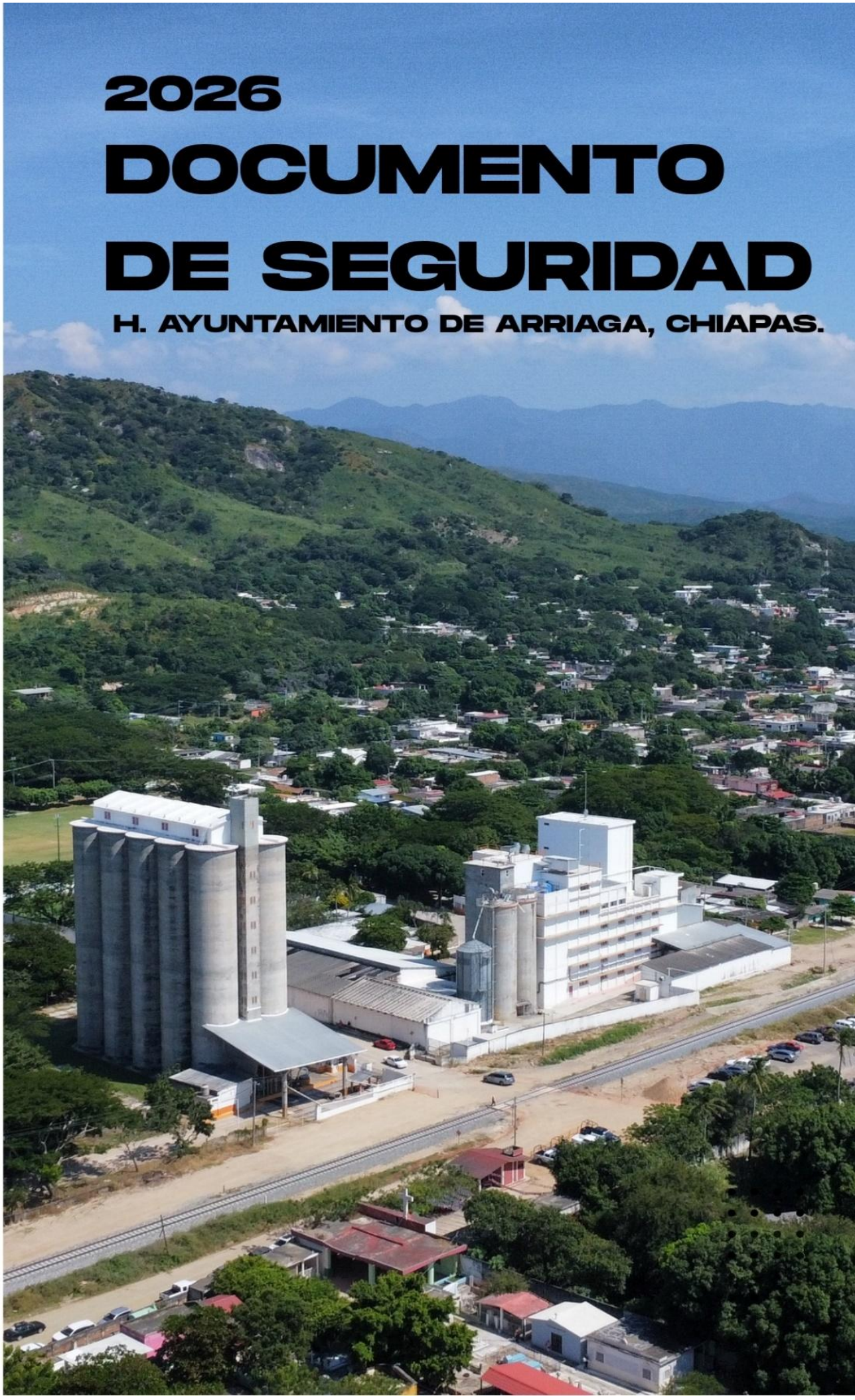
TRANSPARENCIA

TRABAJANDO JUNTOS POR EL MEJOR ARRIAGA DE TODA LA Historia

H. AYUNTAMIENTO 2024 - 2027 ARRIAGA

2026 DOCUMENTO DE SEGURIDAD

H. AYUNTAMIENTO DE ARRIAGA, CHIAPAS.



PRESENTACIÓN

El presente Documento de Seguridad constituye el instrumento rector mediante el cual el H. Ayuntamiento de Arriaga, Chiapas, establece las medidas administrativas, físicas y técnicas necesarias para garantizar la protección de los datos personales que son tratados por las unidades administrativas que integran este sujeto obligado, en cumplimiento de los principios, deberes y obligaciones previstos en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas y demás disposiciones jurídicas aplicables.

Este documento tiene como propósito establecer un Sistema de Gestión de Seguridad de Datos Personales que permita identificar, administrar, proteger, supervisar y mejorar continuamente los procesos relacionados con el tratamiento de los datos personales que obran en posesión del Ayuntamiento, procurando en todo momento su confidencialidad, integridad, disponibilidad y resiliencia frente a cualquier riesgo o vulneración.

Para su elaboración se realizó un análisis de las actividades sustantivas desarrolladas por las distintas unidades administrativas que conforman el H. Ayuntamiento de Arriaga, identificando los tratamientos de datos personales que llevan a cabo en el ejercicio de sus atribuciones, así como los riesgos asociados a dichos tratamientos, con el propósito de implementar medidas de seguridad acordes con la naturaleza de la información resguardada y con las capacidades institucionales del sujeto obligado.

Las medidas de seguridad contenidas en este Documento tienen un enfoque preventivo y de mejora continua, por lo que deberán revisarse y actualizarse cuando ocurran modificaciones relevantes en los tratamientos de datos personales, en la estructura orgánica del Ayuntamiento, en la normatividad aplicable o cuando se identifiquen vulneraciones o riesgos que hagan necesaria su adecuación.

Asimismo, el presente Documento de Seguridad constituye una herramienta de apoyo para las personas servidoras públicas que, en el ejercicio de sus funciones, intervienen en el tratamiento de datos personales, estableciendo criterios claros para su manejo, conservación, acceso, transferencia, resguardo, respaldo, supresión y, en su caso, destrucción, privilegiando en todo momento el respeto al derecho humano de protección de datos personales.

Finalmente, el H. Ayuntamiento de Arriaga, Chiapas, asume el compromiso permanente de fortalecer la cultura institucional de protección de datos personales mediante acciones de capacitación, supervisión, mejora continua y evaluación periódica de las medidas implementadas, promoviendo el cumplimiento de la legislación vigente y de las mejores prácticas en la materia.

OBJETIVO DEL DOCUMENTO DE SEGURIDAD MUNICIPAL

El presente Documento de Seguridad tiene como objetivo establecer las directrices, mecanismos, procedimientos y medidas de seguridad administrativas, físicas y técnicas que permitan garantizar la protección de los datos personales tratados por el H. Ayuntamiento de Arriaga, Chiapas, asegurando que su tratamiento se realice conforme a los principios, deberes y obligaciones establecidos en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas y demás disposiciones jurídicas aplicables.

Asimismo, tiene por objeto implementar un Sistema de Gestión de Seguridad de Datos Personales que permita identificar los tratamientos de datos personales que realizan las unidades administrativas del Ayuntamiento; evaluar los riesgos asociados; establecer controles preventivos y correctivos; atender incidentes de seguridad; fortalecer la cultura institucional en materia de protección de datos personales y promover la mejora continua de las medidas de seguridad implementadas.

Las medidas previstas en este Documento deberán observarse por todas las personas servidoras públicas que intervengan en cualquier etapa del tratamiento de datos personales, con la finalidad de prevenir su alteración, pérdida, destrucción, uso, acceso, divulgación o cualquier tratamiento no autorizado, garantizando en todo momento la protección de los derechos de las personas titulares de los datos personales.

RESPONSABILIDADES Y ATRIBUCIONES

De conformidad con la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, corresponde al H. Ayuntamiento de Arriaga, Chiapas, en su carácter de sujeto obligado, implementar las medidas necesarias para garantizar la protección de los datos personales que obren en su posesión.

El Comité de Transparencia, dentro del ámbito de sus atribuciones legales, fungirá como la instancia colegiada encargada de coordinar y supervisar las acciones institucionales relacionadas con la protección de datos personales, así como de promover la actualización y observancia del presente Documento de Seguridad.

La Unidad de Transparencia, en el ámbito de sus atribuciones, coadyuvará con las unidades administrativas en la implementación, seguimiento, difusión y mejora continua de las medidas previstas en este Documento, brindando asesoría y acompañamiento en materia de protección de datos personales cuando resulte necesario.

Las personas titulares de las unidades administrativas serán responsables de implementar las medidas de seguridad correspondientes dentro de los tratamientos de datos personales que administren, vigilando que el personal adscrito a su área observe las obligaciones previstas en la legislación aplicable y en el presente Documento.

Las personas servidoras públicas que, con motivo de sus funciones, tengan acceso a datos personales deberán:

- Tratar los datos personales exclusivamente para el cumplimiento de las atribuciones que les confiere la normatividad aplicable.
- Guardar absoluta confidencialidad respecto de la información a la que tengan acceso, aun después de concluir su empleo, cargo o comisión, en los casos previstos por la legislación.
- Aplicar las medidas administrativas, físicas y técnicas establecidas para cada tratamiento.
- Informar inmediatamente a la persona titular de su unidad administrativa cualquier incidente o vulneración de seguridad del que tengan conocimiento.
- Participar en las acciones de capacitación y actualización que en materia de protección de datos personales organice el Ayuntamiento.
- Observar las disposiciones contenidas en este Documento de Seguridad y demás normativa aplicable.

La implementación del presente Documento constituye una responsabilidad institucional compartida entre todas las unidades administrativas del H. Ayuntamiento de Arriaga, Chiapas, por lo que cada una deberá adoptar las acciones necesarias para garantizar el cumplimiento de las medidas de seguridad aquí establecidas.

ALCANCE DEL DOCUMENTO DE SEGURIDAD

El presente Documento de Seguridad es de observancia obligatoria para todas las unidades administrativas que integran el H. Ayuntamiento de Arriaga, Chiapas, que en el ejercicio de sus atribuciones realicen cualquier tratamiento de datos personales, independientemente del medio físico o electrónico en que éstos se encuentren.

Las disposiciones contenidas en este Documento serán aplicables a los procesos de obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, transferencia, acceso, almacenamiento, bloqueo, supresión, destrucción y cualquier otra operación realizada respecto de datos personales.

Con base en el inventario institucional de tratamientos de datos personales, las unidades administrativas que actualmente realizan tratamientos de datos personales comprenden, entre otras, las siguientes:

- Órgano Interno de Control.
- Unidad de Transparencia.
- Secretaría del Ayuntamiento.
- Tesorería Municipal.
- Dirección de Recursos Humanos.
- Dirección Jurídica.
- Juzgado Calificador.
- Sistema DIF Municipal.
- Dirección de Salud.

- Dirección de Protección Civil.
- Consejo Municipal de Seguridad Pública.
- Dirección de Derechos Humanos.
- Instituto Municipal de la Mujer.
- SIPINNA.
- Programas Sociales.
- Oficialía Mayor.
- Cualquier otra unidad administrativa que, con motivo del ejercicio de sus atribuciones legales, recabe, utilice, almacene o administre datos personales.

La incorporación de nuevas unidades administrativas o nuevos tratamientos de datos personales no requerirá la emisión de un nuevo Documento de Seguridad; bastará con la actualización del inventario de tratamientos y de las medidas de seguridad correspondientes, conforme al procedimiento de revisión previsto en este documento.

Las medidas de seguridad previstas serán aplicables tanto a los expedientes físicos como a la información contenida en equipos de cómputo, dispositivos electrónicos, bases de datos, sistemas institucionales, servicios de almacenamiento autorizados y cualquier otro medio utilizado para el tratamiento de datos personales.

SISTEMA DE GESTIÓN DE LOS DATOS PERSONALES

El H. Ayuntamiento de Arriaga, Chiapas, implementa un Sistema de Gestión de Seguridad de Datos Personales como el conjunto de políticas, procedimientos, controles, actividades y medidas orientadas a garantizar la protección de los datos personales tratados por las unidades administrativas que integran este sujeto obligado.

El Sistema de Gestión tiene como finalidad establecer mecanismos permanentes que permitan identificar los tratamientos de datos personales, administrar los riesgos asociados, implementar medidas de seguridad, supervisar su cumplimiento y promover la mejora continua de los procesos relacionados con la protección de datos personales.

Su funcionamiento comprende las siguientes etapas:

I. Identificación de los tratamientos de datos personales

Las unidades administrativas deberán identificar permanentemente los tratamientos de datos personales que realicen en ejercicio de sus atribuciones legales.
Para cada tratamiento deberá identificarse, cuando menos:

- Unidad administrativa responsable.
- Nombre del tratamiento.
- Finalidad del tratamiento.
- Categorías de titulares.
- Categorías de datos personales.

- Identificación de datos personales sensibles, en su caso.
- Medio de almacenamiento (físico, electrónico o mixto).
- Servidores públicos autorizados para el tratamiento.
- Transferencias que, en su caso, procedan conforme a la legislación.
- Medidas de seguridad implementadas.

El inventario institucional deberá actualizarse cuando se creen nuevos tratamientos, desaparezcan los existentes o se modifiquen sustancialmente sus finalidades.

II. Identificación y clasificación de los datos personales

Las unidades administrativas deberán identificar los datos personales que recaben y clasificarlos conforme a su naturaleza.

Para efectos del presente Documento se consideran, entre otros:

Datos de identificación

Nombre, domicilio, fotografía, firma, CURP, RFC, fecha y lugar de nacimiento, nacionalidad, estado civil, teléfono, correo electrónico y demás datos de identificación.

Datos laborales

Nombramientos, expedientes laborales, historial administrativo, escolaridad, puesto, remuneraciones y documentación relacionada con el empleo público.

Datos patrimoniales

Información bancaria, cuentas, ingresos, declaraciones patrimoniales y demás información de naturaleza económica cuando resulte procedente.

Datos académicos

Escolaridad, certificados, títulos, constancias y demás antecedentes académicos.

Datos sensibles

Información relacionada con el estado de salud, discapacidad, origen étnico, creencias religiosas, opiniones políticas, afiliación sindical, datos biométricos y cualquier otro dato cuya utilización indebida pueda dar origen a discriminación o implique un riesgo grave para la persona titular.

III. Análisis y administración de riesgos

Para cada tratamiento deberán identificarse los riesgos que puedan afectar la confidencialidad, integridad y disponibilidad de los datos personales.

Entre otros riesgos deberán considerarse:

- Acceso no autorizado.
- Pérdida de información.
- Robo de expedientes.
- Destrucción accidental.
- Modificación indebida.
- Divulgación no autorizada.
- Uso distinto a la finalidad.
- Fallas eléctricas.

- Daños ocasionados por fenómenos naturales.
- Fallas de equipos informáticos.
- Errores humanos.
- Ataques informáticos.
- Uso inadecuado de dispositivos móviles.

Los riesgos identificados servirán de base para determinar las medidas de seguridad que deberán implementarse.

IV. Implementación de medidas de seguridad

Con base en el análisis de riesgos, cada unidad administrativa implementará las medidas administrativas, físicas y técnicas que resulten necesarias para proteger los datos personales.

Las medidas deberán ser razonables, proporcionales al riesgo y acordes con la naturaleza de los tratamientos realizados por el Ayuntamiento.

Cuando se identifique una vulneración o un nuevo riesgo, las medidas deberán revisarse y fortalecerse de manera inmediata.

V. Monitoreo y mejora continua

El Sistema de Gestión será objeto de seguimiento permanente.
Para ello se realizarán, entre otras acciones:

- Revisión periódica del Documento de Seguridad.
- Actualización del inventario de tratamientos.
- Revisión de las medidas implementadas.
- Atención de incidentes de seguridad.
- Seguimiento de las acciones correctivas.
- Capacitación continua.
- Revisión del cumplimiento por parte de las unidades administrativas.

Las observaciones derivadas de auditorías, autoevaluaciones o revisiones internas servirán como base para fortalecer el Sistema de Gestión.

VI. Difusión y cultura institucional

La Unidad de Transparencia promoverá la difusión del presente Documento de Seguridad entre todas las unidades administrativas.
Asimismo, impulsará acciones permanentes de sensibilización y capacitación para fortalecer la cultura institucional en materia de protección de datos personales.
Las personas servidoras públicas deberán conocer las medidas de seguridad aplicables a los tratamientos bajo su responsabilidad y participar en las actividades de capacitación que se programen.

FUNCIONES Y OBLIGACIONES DEL RESPONSABLE, ENCARGADOS Y PERSONAS QUE TRATEN DATOS PERSONALES

Con el propósito de garantizar el adecuado tratamiento de los datos personales y el cumplimiento de las disposiciones legales aplicables, el H. Ayuntamiento de Arriaga, Chiapas, establece las funciones y obligaciones de las personas servidoras públicas que intervienen en cualquier etapa del tratamiento de datos personales.

Las responsabilidades previstas en este apartado son de observancia obligatoria para todas las unidades administrativas que integran el Ayuntamiento y deberán cumplirse atendiendo a las atribuciones conferidas por la legislación aplicable y por el presente Documento de Seguridad.

I. Del Responsable del Tratamiento de los Datos Personales

El H. Ayuntamiento de Arriaga, Chiapas, en su carácter de sujeto obligado, es el responsable del tratamiento de los datos personales que recabe, utilice, almacene, conserve, transfiera o suprima en el ejercicio de sus atribuciones legales.

Para el cumplimiento de esta responsabilidad deberá:

Garantizar que el tratamiento de los datos personales se realice conforme a los principios, deberes y obligaciones previstos en la legislación aplicable.

Implementar y mantener actualizado el presente Documento de Seguridad.

Promover la adopción de medidas administrativas, físicas y técnicas para proteger los datos personales.

Identificar los tratamientos de datos personales que realizan las unidades administrativas.

Promover la actualización permanente del inventario de tratamientos de datos personales.
Supervisar el cumplimiento de las medidas de seguridad establecidas en este Documento.
Garantizar el ejercicio de los derechos que correspondan a las personas titulares de los datos personales.

Establecer mecanismos para atender incidentes de seguridad.

Promover la capacitación permanente de las personas servidoras públicas.
Implementar acciones de mejora continua derivadas de auditorías, autoevaluaciones o revisiones internas.

II. Del Comité de Transparencia

En el ámbito de sus atribuciones legales, el Comité de Transparencia será la instancia encargada de impulsar las acciones institucionales relacionadas con la protección de datos personales.

Corresponderá al Comité de Transparencia:

- Promover la observancia del presente Documento de Seguridad.
- Dar seguimiento a las acciones institucionales relacionadas con la protección de datos personales.
- Conocer de los asuntos que, conforme a la legislación aplicable, sean sometidos a su consideración.
- Promover la actualización del Documento de Seguridad cuando existan modificaciones relevantes en los tratamientos de datos personales o en la normatividad aplicable.
- Impulsar la mejora continua del Sistema de Gestión de Seguridad de Datos Personales.

III. De la Unidad de Transparencia

La Unidad de Transparencia fungirá como instancia de apoyo y coordinación en materia de protección de datos personales.

Le corresponderá:

- Asesorar a las unidades administrativas respecto del cumplimiento de sus obligaciones.
- Coordinar la actualización del Documento de Seguridad.
- Dar seguimiento al inventario institucional de tratamientos de datos personales.
- Promover la elaboración y actualización de los avisos de privacidad.
- Coordinar las actividades de capacitación en materia de protección de datos personales.
- Coadyuvar en la atención de incidentes de seguridad relacionados con datos personales.
- Promover la difusión del presente Documento de Seguridad entre todas las unidades administrativas.

IV. De las personas titulares de las unidades administrativas

Las personas titulares de cada unidad administrativa serán responsables del tratamiento de los datos personales que administren dentro del ámbito de sus atribuciones.

Para ello deberán:

- Garantizar el cumplimiento de las medidas de seguridad previstas en este Documento.
- Vigilar que únicamente el personal autorizado tenga acceso a los datos personales.
- Identificar y documentar los tratamientos de datos personales bajo su responsabilidad.
- Mantener actualizado el inventario de tratamientos correspondiente a su unidad administrativa.
- Informar oportunamente cualquier modificación en los tratamientos de datos personales.
- Reportar de inmediato cualquier incidente de seguridad.
- Promover entre el personal a su cargo el cumplimiento de las medidas de seguridad.
- Facilitar las revisiones y auditorías que se realicen en materia de protección de datos personales.

V. De las personas servidoras públicas que tratan datos personales

Toda persona servidora pública que intervenga en el tratamiento de datos personales deberá:

- Utilizar los datos personales exclusivamente para el cumplimiento de las funciones que tenga legalmente encomendadas.
- Guardar confidencialidad respecto de la información a la que tenga acceso, aun después de concluir su empleo, cargo o comisión, cuando así lo establezca la legislación aplicable.
- Observar las medidas administrativas, físicas y técnicas previstas en este Documento.
- Evitar la reproducción, extracción, copia, fotografía, divulgación o transferencia no autorizada de datos personales.
- Utilizar únicamente los equipos, sistemas y medios institucionales autorizados para el tratamiento de datos personales.
- Reportar inmediatamente cualquier incidente, pérdida, robo, acceso no autorizado o vulneración de seguridad de la que tenga conocimiento.
- Participar en los programas de capacitación y actualización que implemente el Ayuntamiento.
- Colaborar en las acciones de supervisión, revisión y mejora continua del Sistema de Gestión de Seguridad de Datos Personales.

VI. De los Encargados del Tratamiento

Cuando el H. Ayuntamiento de Arriaga, Chiapas, encomiende a una persona física o moral el tratamiento de datos personales mediante la celebración del instrumento jurídico correspondiente, ésta tendrá el carácter de Encargado y deberá observar las obligaciones previstas en la legislación aplicable y en el contrato, convenio o instrumento jurídico que regule dicha relación.
El Encargado deberá, entre otras obligaciones:

- Tratar los datos personales únicamente conforme a las instrucciones del Responsable.
- Implementar las medidas de seguridad acordadas.
- Guardar confidencialidad respecto de los datos personales tratados.
- Abstenerse de utilizar la información para fines distintos a los autorizados.
- Informar cualquier incidente de seguridad que pudiera comprometer los datos personales.
- Suprimir o devolver los datos personales una vez concluido el servicio, cuando así proceda conforme al instrumento jurídico correspondiente.

VII. Obligaciones generales

Todas las personas servidoras públicas del H. Ayuntamiento de Arriaga, Chiapas, deberán contribuir al fortalecimiento del Sistema de Gestión de Seguridad de Datos Personales, observando permanentemente las medidas de seguridad previstas en este Documento y promoviendo una cultura institucional de protección de datos personales basada en la legalidad, responsabilidad, confidencialidad, integridad, disponibilidad y mejora continua.

RESGUARDO DE LOS SOPORTES FÍSICOS Y/O ELECTRÓNICOS DE LOS DATOS PERSONALES
Con la finalidad de garantizar la confidencialidad, integridad y disponibilidad de los datos personales que obran en posesión del H. Ayuntamiento de Arriaga, Chiapas, las unidades administrativas deberán implementar las medidas necesarias para proteger los soportes físicos y electrónicos que contengan información con datos personales, considerando la naturaleza de los tratamientos que realizan y los riesgos asociados.
Las medidas previstas en este apartado serán de observancia obligatoria para todas las personas servidoras públicas que intervengan en el tratamiento de datos personales.

I. Resguardo de soportes físicos
Los expedientes, documentos, archivos, libros de registro, formatos, copias certificadas y cualquier otro soporte físico que contenga datos personales deberán observar, cuando menos, las siguientes medidas:

- Permanecer bajo resguardo de la unidad administrativa responsable.

- Conservarse en archiveros, gavetas, oficinas o espacios que permitan limitar el acceso únicamente al personal autorizado.
- Evitar que la documentación permanezca expuesta al público o en lugares de libre acceso.
- Mantener un adecuado orden y clasificación documental que facilite su localización y evite pérdidas o extravíos.
- Cuando un expediente sea consultado por personal autorizado, deberá devolverse al lugar destinado para su resguardo al concluir su utilización.
- En caso de traslado de expedientes entre unidades administrativas, éste deberá realizarse procurando su integridad y evitando el acceso por personas no autorizadas.

II. Resguardo de soportes electrónicos

Los equipos de cómputo, discos duros, memorias USB institucionales, servidores, bases de datos, equipos portátiles y demás dispositivos electrónicos que almacenen datos personales deberán contar, cuando menos, con las siguientes medidas:

- Acceso mediante usuario y contraseña.
- Cambio periódico de contraseñas cuando existan riesgos de seguridad o rotación del personal autorizado.
- Uso de software antivirus actualizado.
- Restricción de instalación de programas no autorizados relacionados con el tratamiento institucional de información.
- Respaldo periódico de la información conforme a las posibilidades técnicas del Ayuntamiento.
- Cierre de sesión cuando el equipo permanezca sin supervisión.
- Evitar almacenar datos personales en dispositivos particulares no autorizados por el Ayuntamiento.

III. Acceso a la información

El acceso a los datos personales únicamente podrá ser realizado por las personas servidoras públicas que, con motivo de sus funciones, requieran conocer dicha información.

Cada unidad administrativa será responsable de identificar al personal autorizado para acceder a los tratamientos bajo su resguardo.

Cuando concluya la relación laboral, cambien las funciones del personal o dejen de existir las necesidades de acceso, deberán retirarse los permisos correspondientes y recuperarse, en su caso, los expedientes, dispositivos o documentos institucionales asignados.

IV. Traslado de información

Cuando resulte necesario trasladar expedientes o dispositivos que contengan datos personales, deberán observarse las siguientes medidas:

- El traslado deberá obedecer exclusivamente a necesidades institucionales.

- Se procurará que la documentación permanezca bajo supervisión del personal responsable durante todo el traslado.
- Deberán evitarse pérdidas, extravíos o accesos no autorizados.
- En caso de utilizar medios electrónicos para remitir información entre unidades administrativas, deberán emplearse preferentemente los medios institucionales autorizados.

V. Conservación y disposición documental

Los expedientes que contengan datos personales deberán conservarse conforme a los plazos establecidos en el Catálogo de Disposición Documental, el Cuadro General de Clasificación Archivística y demás instrumentos archivísticos aplicables.

Una vez concluido el plazo de conservación y siempre que exista fundamento para ello, la disposición final de la documentación deberá realizarse conforme a la normatividad archivística vigente, procurando que los datos personales no puedan ser recuperados por personas no autorizadas.

VI. Medidas ante incidentes

Cuando se detecte la pérdida, robo, extravío, destrucción, acceso no autorizado o cualquier otra situación que pudiera comprometer la seguridad de los datos personales contenidos en soportes físicos o electrónicos, la persona servidora pública que tenga conocimiento deberá informar inmediatamente a la persona titular de su unidad administrativa y a la Unidad de Transparencia para que se implementen las acciones de contención, análisis, documentación y, en su caso, las medidas correctivas correspondientes.

BITÁCORAS DE ACCESO, OPERACIÓN COTIDIANA Y VULNERACIONES A LA SEGURIDAD DE LOS DATOS PERSONALES

Con el propósito de fortalecer la trazabilidad de los tratamientos de datos personales y facilitar la identificación de incidentes de seguridad, las unidades administrativas implementarán mecanismos de registro acordes con la naturaleza de los tratamientos que realizan.

Cuando las características del tratamiento lo permitan, deberán conservarse registros relacionados con:

I. Bitácoras de acceso

Se registrarán, cuando resulte procedente:

- Fecha del acceso.
- Persona servidora pública que accedió.
- Expediente, sistema o información consultada.
- Motivo del acceso, cuando sea necesario.

En los tratamientos que por su naturaleza no permitan llevar una bitácora formal, la unidad administrativa deberá implementar mecanismos razonables de control de acceso.

II. Bitácoras de operación

Las unidades administrativas podrán documentar las actividades relevantes relacionadas con el tratamiento de datos personales, tales como:

- Incorporación de nuevos expedientes.
- Actualización de información.
- Corrección de datos.
- Transferencias autorizadas.
- Respaldo de información.
- Supresión o disposición final.

Estos registros permitirán identificar las acciones realizadas sobre los tratamientos y facilitarán la supervisión institucional.

III. Registro de vulneraciones de seguridad

Toda vulneración de seguridad relacionada con datos personales deberá documentarse mediante un registro interno que contenga, cuando menos:

- Fecha del incidente.
- Unidad administrativa involucrada.
- Descripción de los hechos.
- Tipo de vulneración.
- Datos personales posiblemente comprometidos.
- Medidas de contención implementadas.
- Acciones correctivas adoptadas.
- Seguimiento realizado.
- Fecha de conclusión del incidente.

La documentación de estos incidentes permitirá fortalecer el análisis de riesgos y mejorar las medidas de seguridad implementadas por el Ayuntamiento.

ANÁLISIS DE RIESGOS Y BRECHA

Sección Clasificada del Documento de Seguridad, apartado del Análisis de Riesgo y Brecha.

Se testa el apartado número 6, que contiene el Análisis de Riesgo y Brecha, contiene información que identifica las vulnerabilidades, debilidades, amenazas y deficiencias de las medidas de seguridad implementadas por el sujeto obligado. Su divulgación podría facilitar accesos no autorizados, vulneraciones de datos personales o afectar la eficacia de los controles de seguridad, de conformidad con lo dispuesto en los artículos 103, fracción II, 112 fracción VI, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas y en los artículos 3, fracción IX, y 6, párrafo primero, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, así como en el artículo vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.

Sección Clasificada del Documento de Seguridad, apartado del Análisis de Riesgo y Brecha.

Se testa el apartado número 6, que contiene el Análisis de Riesgo y Brecha, contiene información que identifica las vulnerabilidades, debilidades, amenazas y deficiencias de las medidas de seguridad implementadas por el sujeto obligado. Su divulgación podría facilitar accesos no autorizados, vulneraciones de datos personales o afectar la eficacia de los controles de seguridad, de conformidad con lo dispuesto en los artículos 103, fracción II, 112 fracción VI, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas y en los artículos 3, fracción IX, y 6, párrafo primero, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, así como en el artículo vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.

Sección Clasificada del Documento de Seguridad, apartado del Análisis de Riesgo y Brecha.

Se testa el apartado número 6, que contiene el Análisis de Riesgo y Brecha, contiene información que identifica las vulnerabilidades, debilidades, amenazas y deficiencias de las medidas de seguridad implementadas por el sujeto obligado. Su divulgación podría facilitar accesos no autorizados, vulneraciones de datos personales o afectar la eficacia de los controles de seguridad, de conformidad con lo dispuesto en los artículos 103, fracción II, 112 fracción VI, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas y en los artículos 3, fracción IX, y 6, párrafo primero, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, así como en el artículo vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.

Sección Clasificada del Documento de Seguridad, apartado del Análisis de Riesgo y Brecha.

Se testa el apartado número 6, que contiene el Análisis de Riesgo y Brecha, contiene información que identifica las vulnerabilidades, debilidades, amenazas y deficiencias de las medidas de seguridad implementadas por el sujeto obligado. Su divulgación podría facilitar accesos no autorizados, vulneraciones de datos personales o afectar la eficacia de los controles de seguridad, de conformidad con lo dispuesto en los artículos 103, fracción II, 112 fracción VI, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas y en los artículos 3, fracción IX, y 6, párrafo primero, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, así como en el artículo vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.

Sección Clasificada del Documento de Seguridad, apartado del Análisis de Riesgo y Brecha.

Se testa el apartado número 6, que contiene el Análisis de Riesgo y Brecha, contiene información que identifica las vulnerabilidades, debilidades, amenazas y deficiencias de las medidas de seguridad implementadas por el sujeto obligado. Su divulgación podría facilitar accesos no autorizados, vulneraciones de datos personales o afectar la eficacia de los controles de seguridad, de conformidad con lo dispuesto en los artículos 103, fracción II, 112 fracción VI, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas y en los artículos 3, fracción IX, y 6, párrafo primero, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, así como en el artículo vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.

Sección Clasificada del Documento de Seguridad, apartado del Análisis de Riesgo y Brecha.

Se testa el apartado número 6, que contiene el Análisis de Riesgo y Brecha, contiene información que identifica las vulnerabilidades, debilidades, amenazas y deficiencias de las medidas de seguridad implementadas por el sujeto obligado. Su divulgación podría facilitar accesos no autorizados, vulneraciones de datos personales o afectar la eficacia de los controles de seguridad, de conformidad con lo dispuesto en los artículos 103, fracción II, 112 fracción VI, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas y en los artículos 3, fracción IX, y 6, párrafo primero, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, así como en el artículo vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.

Sección Clasificada del Documento de Seguridad, apartado del Análisis de Riesgo y Brecha.

Se testa el apartado número 6, que contiene el Análisis de Riesgo y Brecha, contiene información que identifica las vulnerabilidades, debilidades, amenazas y deficiencias de las medidas de seguridad implementadas por el sujeto obligado. Su divulgación podría facilitar accesos no autorizados, vulneraciones de datos personales o afectar la eficacia de los controles de seguridad, de conformidad con lo dispuesto en los artículos 103, fracción II, 112 fracción VI, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas y en los artículos 3, fracción IX, y 6, párrafo primero, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, así como en el artículo vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.

Sección Clasificada del Documento de Seguridad, apartado del Análisis de Riesgo y Brecha.

Se testa el apartado número 6, que contiene el Análisis de Riesgo y Brecha, contiene información que identifica las vulnerabilidades, debilidades, amenazas y deficiencias de las medidas de seguridad implementadas por el sujeto obligado. Su divulgación podría facilitar accesos no autorizados, vulneraciones de datos personales o afectar la eficacia de los controles de seguridad, de conformidad con lo dispuesto en los artículos 103, fracción II, 112 fracción VI, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas y en los artículos 3, fracción IX, y 6, párrafo primero, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, así como en el artículo vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.

Sección Clasificada del Documento de Seguridad, apartado del Análisis de Riesgo y Brecha.

Se testa el apartado número 6, que contiene el Análisis de Riesgo y Brecha, contiene información que identifica las vulnerabilidades, debilidades, amenazas y deficiencias de las medidas de seguridad implementadas por el sujeto obligado. Su divulgación podría facilitar accesos no autorizados, vulneraciones de datos personales o afectar la eficacia de los controles de seguridad, de conformidad con lo dispuesto en los artículos 103, fracción II, 112 fracción VI, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas y en los artículos 3, fracción IX, y 6, párrafo primero, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, así como en el artículo vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.

Sección Clasificada del Documento de Seguridad, apartado del Análisis de Riesgo y Brecha.

Se testa el apartado número 6, que contiene el Análisis de Riesgo y Brecha, contiene información que identifica las vulnerabilidades, debilidades, amenazas y deficiencias de las medidas de seguridad implementadas por el sujeto obligado. Su divulgación podría facilitar accesos no autorizados, vulneraciones de datos personales o afectar la eficacia de los controles de seguridad, de conformidad con lo dispuesto en los artículos 103, fracción II, 112 fracción VI, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas y en los artículos 3, fracción IX, y 6, párrafo primero, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, así como en el artículo vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.

Sección Clasificada del Documento de Seguridad, apartado del Análisis de Riesgo y Brecha.

Se testa el apartado número 6, que contiene el Análisis de Riesgo y Brecha, contiene información que identifica las vulnerabilidades, debilidades, amenazas y deficiencias de las medidas de seguridad implementadas por el sujeto obligado. Su divulgación podría facilitar accesos no autorizados, vulneraciones de datos personales o afectar la eficacia de los controles de seguridad, de conformidad con lo dispuesto en los artículos 103, fracción II, 112 fracción VI, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas y en los artículos 3, fracción IX, y 6, párrafo primero, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, así como en el artículo vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.

Sección Clasificada del Documento de Seguridad, apartado del Análisis de Riesgo y Brecha.

Se testa el apartado número 6, que contiene el Análisis de Riesgo y Brecha, contiene información que identifica las vulnerabilidades, debilidades, amenazas y deficiencias de las medidas de seguridad implementadas por el sujeto obligado. Su divulgación podría facilitar accesos no autorizados, vulneraciones de datos personales o afectar la eficacia de los controles de seguridad, de conformidad con lo dispuesto en los artículos 103, fracción II, 112 fracción VI, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas y en los artículos 3, fracción IX, y 6, párrafo primero, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, así como en el artículo vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.

Sección Clasificada del Documento de Seguridad, apartado del Análisis de Riesgo y Brecha.

Se testa el apartado número 6, que contiene el Análisis de Riesgo y Brecha, contiene información que identifica las vulnerabilidades, debilidades, amenazas y deficiencias de las medidas de seguridad implementadas por el sujeto obligado. Su divulgación podría facilitar accesos no autorizados, vulneraciones de datos personales o afectar la eficacia de los controles de seguridad, de conformidad con lo dispuesto en los artículos 103, fracción II, 112 fracción VI, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas y en los artículos 3, fracción IX, y 6, párrafo primero, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, así como en el artículo vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.

Sección Clasificada del Documento de Seguridad, apartado del Análisis de Riesgo y Brecha.

Se testa el apartado número 6, que contiene el Análisis de Riesgo y Brecha, contiene información que identifica las vulnerabilidades, debilidades, amenazas y deficiencias de las medidas de seguridad implementadas por el sujeto obligado. Su divulgación podría facilitar accesos no autorizados, vulneraciones de datos personales o afectar la eficacia de los controles de seguridad, de conformidad con lo dispuesto en los artículos 103, fracción II, 112 fracción VI, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas y en los artículos 3, fracción IX, y 6, párrafo primero, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, así como en el artículo vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.

Sección Clasificada del Documento de Seguridad, apartado del Análisis de Riesgo y Brecha.

Se testa el apartado número 6, que contiene el Análisis de Riesgo y Brecha, contiene información que identifica las vulnerabilidades, debilidades, amenazas y deficiencias de las medidas de seguridad implementadas por el sujeto obligado. Su divulgación podría facilitar accesos no autorizados, vulneraciones de datos personales o afectar la eficacia de los controles de seguridad, de conformidad con lo dispuesto en los artículos 103, fracción II, 112 fracción VI, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas y en los artículos 3, fracción IX, y 6, párrafo primero, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, así como en el artículo vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.

Sección Clasificada del Documento de Seguridad, apartado del Análisis de Riesgo y Brecha.

Se testa el apartado número 6, que contiene el Análisis de Riesgo y Brecha, contiene información que identifica las vulnerabilidades, debilidades, amenazas y deficiencias de las medidas de seguridad implementadas por el sujeto obligado. Su divulgación podría facilitar accesos no autorizados, vulneraciones de datos personales o afectar la eficacia de los controles de seguridad, de conformidad con lo dispuesto en los artículos 103, fracción II, 112 fracción VI, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas y en los artículos 3, fracción IX, y 6, párrafo primero, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, así como en el artículo vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.

Sección Clasificada del Documento de Seguridad, apartado del Análisis de Riesgo y Brecha.

Se testa el apartado número 6, que contiene el Análisis de Riesgo y Brecha, contiene información que identifica las vulnerabilidades, debilidades, amenazas y deficiencias de las medidas de seguridad implementadas por el sujeto obligado. Su divulgación podría facilitar accesos no autorizados, vulneraciones de datos personales o afectar la eficacia de los controles de seguridad, de conformidad con lo dispuesto en los artículos 103, fracción II, 112 fracción VI, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas y en los artículos 3, fracción IX, y 6, párrafo primero, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, así como en el artículo vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.

MATRIZ DE ANÁLISIS DE LA INFORMACIÓN

Sección Clasificada del Documento de Seguridad, apartado del Análisis de Riesgo y Brecha.

Se testa el apartado número 6, que contiene el Análisis de Riesgo y Brecha, contiene información que identifica las vulnerabilidades, debilidades, amenazas y deficiencias de las medidas de seguridad implementadas por el sujeto obligado. Su divulgación podría facilitar accesos no autorizados, vulneraciones de datos personales o afectar la eficacia de los controles de seguridad, de conformidad con lo dispuesto en los artículos 103, fracción II, 112 fracción VI, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas y en los artículos 3, fracción IX, y 6, párrafo primero, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, así como en el artículo vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.

Sección Clasificada del Documento de Seguridad, apartado del Análisis de Riesgo y Brecha.

Se testa el apartado número 6, que contiene el Análisis de Riesgo y Brecha, contiene información que identifica las vulnerabilidades, debilidades, amenazas y deficiencias de las medidas de seguridad implementadas por el sujeto obligado. Su divulgación podría facilitar accesos no autorizados, vulneraciones de datos personales o afectar la eficacia de los controles de seguridad, de conformidad con lo dispuesto en los artículos 103, fracción II, 112 fracción VI, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas y en los artículos 3, fracción IX, y 6, párrafo primero, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, así como en el artículo vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.

Sección Clasificada del Documento de Seguridad, apartado del Análisis de Riesgo y Brecha.

Se testa el apartado número 6, que contiene el Análisis de Riesgo y Brecha, contiene información que identifica las vulnerabilidades, debilidades, amenazas y deficiencias de las medidas de seguridad implementadas por el sujeto obligado. Su divulgación podría facilitar accesos no autorizados, vulneraciones de datos personales o afectar la eficacia de los controles de seguridad, de conformidad con lo dispuesto en los artículos 103, fracción II, 112 fracción VI, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas y en los artículos 3, fracción IX, y 6, párrafo primero, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, así como en el artículo vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.

Leyenda de clasificación del nivel de riesgo:

- **Muy Alto:** Datos cuya pérdida, alteración o acceso no autorizado puede causar un daño significativo a la persona afectada o a la institución, incluyendo riesgos financieros, legales y reputacionales graves.
- **Alto:** Datos sensibles cuya exposición puede tener consecuencias serias, aunque no necesariamente devastadoras para las personas o la organización.
- **Medio:** Datos importantes, pero cuyo riesgo y consecuencias de una brecha de seguridad son menos graves en comparación con los de mayor nivel.
- **Bajo:** Datos cuya exposición no tendría un impacto significativo en la seguridad o en la operación de la institución.

Valoración de la información

Del análisis efectuado se concluye que la mayor concentración de información con nivel de riesgo **Alto** y **Muy Alto** corresponde a las unidades administrativas que tratan datos personales sensibles, datos financieros, expedientes laborales, información jurídica, datos de salud, información relacionada con niñas, niños y adolescentes, personas en situación de vulnerabilidad y procedimientos administrativos.

En consecuencia, dichas unidades administrativas deberán mantener controles reforzados para el acceso, conservación, resguardo, transferencia y, en su caso, disposición final de la información bajo su responsabilidad.

Revisión y actualización

El presente análisis deberá revisarse cuando:

- Se incorporen nuevos tratamientos de datos personales.
- Se modifique la estructura orgánica del Ayuntamiento.
- Existan reformas a la legislación aplicable.
- Se identifiquen nuevos riesgos o vulnerabilidades.
- Se implementen nuevos sistemas de información.
- Se deriven observaciones de auditorías, verificaciones o autoevaluaciones.

La actualización de este análisis permitirá mantener vigentes las medidas de seguridad implementadas y fortalecer el Sistema de Gestión de Seguridad de Datos Personales del H. Ayuntamiento de Arriaga, Chiapas.

GESTIÓN DE VULNERACIONES A LA SEGURIDAD DE LOS DATOS PERSONALES

Sección Clasificada del Documento de Seguridad, apartado del Análisis de Riesgo y Brecha.

Se testa el apartado número 6, que contiene el Análisis de Riesgo y Brecha, contiene información que identifica las vulnerabilidades, debilidades, amenazas y deficiencias de las medidas de seguridad implementadas por el sujeto obligado. Su divulgación podría facilitar accesos no autorizados, vulneraciones de datos personales o afectar la eficacia de los controles de seguridad, de conformidad con lo dispuesto en los artículos 103, fracción II, 112 fracción VI, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas y en los artículos 3, fracción IX, y 6, párrafo primero, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, así como en el artículo vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.

Sección Clasificada del Documento de Seguridad, apartado del Análisis de Riesgo y Brecha.

Se testa el apartado número 6, que contiene el Análisis de Riesgo y Brecha, contiene información que identifica las vulnerabilidades, debilidades, amenazas y deficiencias de las medidas de seguridad implementadas por el sujeto obligado. Su divulgación podría facilitar accesos no autorizados, vulneraciones de datos personales o afectar la eficacia de los controles de seguridad, de conformidad con lo dispuesto en los artículos 103, fracción II, 112 fracción VI, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas y en los artículos 3, fracción IX, y 6, párrafo primero, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, así como en el artículo vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.

Sección Clasificada del Documento de Seguridad, apartado del Análisis de Riesgo y Brecha.

Se testa el apartado número 6, que contiene el Análisis de Riesgo y Brecha, contiene información que identifica las vulnerabilidades, debilidades, amenazas y deficiencias de las medidas de seguridad implementadas por el sujeto obligado. Su divulgación podría facilitar accesos no autorizados, vulneraciones de datos personales o afectar la eficacia de los controles de seguridad, de conformidad con lo dispuesto en los artículos 103, fracción II, 112 fracción VI, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas y en los artículos 3, fracción IX, y 6, párrafo primero, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, así como en el artículo vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.

MEDIDAS DE SEGURIDAD ADMINISTRATIVAS, FÍSICAS Y TÉCNICAS

Sección Clasificada del Documento de Seguridad, apartado del Análisis de Riesgo y Brecha.

Se testa el apartado número 6, que contiene el Análisis de Riesgo y Brecha, contiene información que identifica las vulnerabilidades, debilidades, amenazas y deficiencias de las medidas de seguridad implementadas por el sujeto obligado. Su divulgación podría facilitar accesos no autorizados, vulneraciones de datos personales o afectar la eficacia de los controles de seguridad, de conformidad con lo dispuesto en los artículos 103, fracción II, 112 fracción VI, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas y en los artículos 3, fracción IX, y 6, párrafo primero, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, así como en el artículo vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.

Sección Clasificada del Documento de Seguridad, apartado del Análisis de Riesgo y Brecha.

Se testa el apartado número 6, que contiene el Análisis de Riesgo y Brecha, contiene información que identifica las vulnerabilidades, debilidades, amenazas y deficiencias de las medidas de seguridad implementadas por el sujeto obligado. Su divulgación podría facilitar accesos no autorizados, vulneraciones de datos personales o afectar la eficacia de los controles de seguridad, de conformidad con lo dispuesto en los artículos 103, fracción II, 112 fracción VI, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas y en los artículos 3, fracción IX, y 6, párrafo primero, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, así como en el artículo vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.

CONTROLES DE IDENTIFICACIÓN Y AUTENTICACIÓN DE USUARIOS

Sección Clasificada del Documento de Seguridad, apartado del Análisis de Riesgo y Brecha.

Se testa el apartado número 6, que contiene el Análisis de Riesgo y Brecha, contiene información que identifica las vulnerabilidades, debilidades, amenazas y deficiencias de las medidas de seguridad implementadas por el sujeto obligado. Su divulgación podría facilitar accesos no autorizados, vulneraciones de datos personales o afectar la eficacia de los controles de seguridad, de conformidad con lo dispuesto en los artículos 103, fracción II, 112 fracción VI, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas y en los artículos 3, fracción IX, y 6, párrafo primero, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, así como en el artículo vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.

Sección Clasificada del Documento de Seguridad, apartado del Análisis de Riesgo y Brecha.

Se testa el apartado número 6, que contiene el Análisis de Riesgo y Brecha, contiene información que identifica las vulnerabilidades, debilidades, amenazas y deficiencias de las medidas de seguridad implementadas por el sujeto obligado. Su divulgación podría facilitar accesos no autorizados, vulneraciones de datos personales o afectar la eficacia de los controles de seguridad, de conformidad con lo dispuesto en los artículos 103, fracción II, 112 fracción VI, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas y en los artículos 3, fracción IX, y 6, párrafo primero, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, así como en el artículo vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.

Sección Clasificada del Documento de Seguridad, apartado del Análisis de Riesgo y Brecha.

Se testa el apartado número 6, que contiene el Análisis de Riesgo y Brecha, contiene información que identifica las vulnerabilidades, debilidades, amenazas y deficiencias de las medidas de seguridad implementadas por el sujeto obligado. Su divulgación podría facilitar accesos no autorizados, vulneraciones de datos personales o afectar la eficacia de los controles de seguridad, de conformidad con lo dispuesto en los artículos 103, fracción II, 112 fracción VI, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas y en los artículos 3, fracción IX, y 6, párrafo primero, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, así como en el artículo vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.

Sección Clasificada del Documento de Seguridad, apartado del Análisis de Riesgo y Brecha.

Se testa el apartado número 6, que contiene el Análisis de Riesgo y Brecha, contiene información que identifica las vulnerabilidades, debilidades, amenazas y deficiencias de las medidas de seguridad implementadas por el sujeto obligado. Su divulgación podría facilitar accesos no autorizados, vulneraciones de datos personales o afectar la eficacia de los controles de seguridad, de conformidad con lo dispuesto en los artículos 103, fracción II, 112 fracción VI, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas y en los artículos 3, fracción IX, y 6, párrafo primero, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, así como en el artículo vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.

Sección Clasificada del Documento de Seguridad, apartado del Análisis de Riesgo y Brecha.

Se testa el apartado número 6, que contiene el Análisis de Riesgo y Brecha, contiene información que identifica las vulnerabilidades, debilidades, amenazas y deficiencias de las medidas de seguridad implementadas por el sujeto obligado. Su divulgación podría facilitar accesos no autorizados, vulneraciones de datos personales o afectar la eficacia de los controles de seguridad, de conformidad con lo dispuesto en los artículos 103, fracción II, 112 fracción VI, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas y en los artículos 3, fracción IX, y 6, párrafo primero, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, así como en el artículo vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.

PLAN DE CONTINGENCIA

Sección Clasificada del Documento de Seguridad, apartado de Gestión y Plan de Contingencia.

Se testa el apartado número 7, que contiene la Gestión de Vulneraciones y Plan de contingencia, toda vez que contiene información sensible sobre la forma en que el sujeto obligado previene, detecta, contiene, responde y recupera la operación ante incidentes de seguridad, de conformidad con lo dispuesto en los artículos 103, fracción II, 112 fracción VI, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas y en los artículos 3, fracción IX, y 6, párrafo primero, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, así como en el artículo vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.

Sección Clasificada del Documento de Seguridad, apartado de Gestión y Plan de Contingencia.

Se testa el apartado número 7, que contiene la Gestión de Vulneraciones y Plan de contingencia, toda vez que contiene información sensible sobre la forma en que el sujeto obligado previene, detecta, contiene, responde y recupera la operación ante incidentes de seguridad, de conformidad con lo dispuesto en los artículos 103, fracción II, 112 fracción VI, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas y en los artículos 3, fracción IX, y 6, párrafo primero, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, así como en el artículo vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.

Sección Clasificada del Documento de Seguridad, apartado de Gestión y Plan de Contingencia.

Se testa el apartado número 7, que contiene la Gestión de Vulneraciones y Plan de contingencia, toda vez que contiene información sensible sobre la forma en que el sujeto obligado previene, detecta, contiene, responde y recupera la operación ante incidentes de seguridad, de conformidad con lo dispuesto en los artículos 103, fracción II, 112 fracción VI, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas y en los artículos 3, fracción IX, y 6, párrafo primero, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, así como en el artículo vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.

TÉCNICAS UTILIZADAS PARA LA SUPRESIÓN Y BORRADO SEGURO DE LOS DATOS PERSONALES

Objetivo

El presente apartado tiene por objeto establecer las técnicas, procedimientos y controles que deberán observar las unidades administrativas del H. Ayuntamiento de Arriaga, Chiapas, para realizar la supresión, destrucción o borrado seguro de los datos personales, garantizando que, una vez concluido su tratamiento conforme a la legislación aplicable, la información no pueda ser recuperada, reconstruida o utilizada de manera indebida.

La supresión de datos personales deberá realizarse observando las disposiciones previstas en la legislación en materia de protección de datos personales, archivos, transparencia y demás ordenamientos jurídicos aplicables.

I. Principios aplicables a la supresión de datos personales

La supresión o destrucción de datos personales deberá observar los siguientes principios:

- Legalidad.
- Finalidad.
- Confidencialidad.
- Seguridad.
- Disponibilidad.
- Responsabilidad.
- Conservación documental.
- Trazabilidad del procedimiento.

En ningún caso podrán destruirse documentos o información sujetos a conservación obligatoria conforme a la legislación archivística vigente.

II. Procedencia de la supresión

La supresión únicamente procederá cuando concurra alguno de los siguientes supuestos:

- Haya concluido la finalidad que motivó el tratamiento.
- Haya vencido el plazo de conservación documental.
- Exista dictamen de disposición documental cuando corresponda.
- Lo determine una disposición legal.
- Proceda conforme a los instrumentos archivísticos del Ayuntamiento.
- Se trate de copias de trabajo o documentos de apoyo informativo cuya eliminación resulte procedente.

Antes de efectuar cualquier supresión deberá verificarse que la información no forme parte de:

- Procedimientos administrativos pendientes.
- Procedimientos jurisdiccionales.
- Auditorías.
- Recursos de revisión.
- Procedimientos de responsabilidades administrativas.
- Obligaciones de conservación documental.

III. Técnicas para la supresión de documentos físicos

Cuando la información se encuentre contenida en soportes físicos podrán emplearse, entre otras, las siguientes técnicas:

- Triturado mecánico.
- Desintegración del papel.
- Destrucción mediante maquinaria especializada.
- Incineración cuando la legislación aplicable lo permita.
- Entrega a empresa autorizada para destrucción confidencial de documentos.
- Cualquier otro procedimiento que imposibilite razonablemente la reconstrucción de la información.

La documentación deberá permanecer bajo supervisión del personal autorizado durante todo el procedimiento de destrucción.

IV. Técnicas para el borrado seguro de información electrónica

Tratándose de información contenida en medios electrónicos deberán emplearse procedimientos que impidan razonablemente la recuperación posterior de los datos personales.

Podrán utilizarse, entre otros:

- Eliminación segura de archivos.
- Sobrescritura de la información.
- Formateo seguro.
- Restablecimiento de fábrica cuando proceda.
- Desmagnetización de medios de almacenamiento, cuando técnicamente resulte aplicable.
- Destrucción física del dispositivo cuando haya concluido su vida útil.

Antes de reutilizar un dispositivo institucional deberá verificarse que toda la información haya sido eliminada de forma segura.

V. Baja de equipos y dispositivos electrónicos

Cuando un equipo de cómputo, disco duro, memoria USB, servidor, teléfono institucional o cualquier otro dispositivo que haya almacenado datos personales sea dado de baja, transferido, donado, sustituido o destruido, deberá verificarse previamente que la información contenida haya sido eliminada mediante técnicas de borrado seguro.

La baja administrativa del equipo deberá documentarse conforme a los procedimientos patrimoniales y de control interno del Ayuntamiento.

VI. Registro de supresión y borrado seguro

Toda supresión o destrucción de datos personales deberá documentarse mediante un registro institucional.

El registro contendrá, cuando menos:

- Número de folio.
- Fecha.
- Unidad administrativa responsable.
- Descripción de la información eliminada.
- Medio de almacenamiento.
- Fundamento de la supresión.
- Técnica utilizada.
- Persona servidora pública responsable.
- Observaciones.

La Unidad de Transparencia podrá verificar la existencia de dichos registros cuando resulte procedente.

VII. Supervisión del procedimiento

Las personas titulares de las unidades administrativas serán responsables de supervisar que las técnicas de supresión sean aplicadas correctamente.

La Unidad de Transparencia podrá realizar revisiones aleatorias para verificar el cumplimiento del presente procedimiento y emitir recomendaciones de mejora cuando resulte necesario.

VIII. Revisión y mejora continua

Las técnicas utilizadas para la supresión y borrado seguro deberán revisarse cuando:

- Se incorporen nuevos medios de almacenamiento.

- Se implementen nuevas tecnologías.
- Se modifique la legislación aplicable.
- Se detecten vulneraciones relacionadas con información eliminada.
- Se deriven observaciones de auditorías o autoevaluaciones.
- Se actualice el presente Documento de Seguridad.

Las modificaciones que resulten necesarias deberán integrarse al Sistema de Gestión de Seguridad de Datos Personales.

FORMATO DS-01

REGISTRO DE SUPRESIÓN Y BORRADO SEGURO DE DATOS PERSONALES

Folio	Fecha	Unidad Administrativa	Tipo de información eliminada	Soporte (Físico/Electrónico)	Técnica utilizada	Fundamento de la supresión	Responsable	Observaciones

ACTA DE SUPRESIÓN DE DATOS PERSONALES

Cuando la destrucción comprenda expedientes completos, bases de datos o volúmenes importantes de información, la unidad administrativa podrá levantar un **Acta de Supresión de Datos Personales**, en la que se hará constar:

- Fecha y lugar de la diligencia.
- Unidad administrativa responsable.
- Relación de la documentación o información suprimida.
- Fundamento jurídico.
- Técnica de destrucción empleada.
- Nombre y cargo de las personas servidoras públicas que intervinieron.
- Observaciones relevantes.
- Firmas de quienes participaron.

MATRIZ DE TÉCNICAS DE SUPRESIÓN

Tipo de soporte	Técnica recomendada	Nivel de seguridad
Expedientes físicos	Triturado mecánico	Alto
Expedientes físicos	Desintegración	Alto
Discos duros	Sobrescritura y formateo seguro	Alto
Memorias USB	Formateo seguro y sobrescritura	Alto
Equipos de cómputo dados de baja	Borrado seguro previo a su disposición	Alto
Discos ópticos	Destrucción física	Alto
Copias simples	Triturado	Medio

PLAN DE TRABAJO PARA LA IMPLEMENTACIÓN DE MEDIDAS DE SEGURIDAD

Sección Clasificada del Documento de Seguridad, apartado del Plan de Trabajo.

Se testa el apartado número 9, que contiene el Plan de Trabajo, en virtud de ser un instrumento de gestión que deriva del análisis de riesgo y del análisis de brecha, en él se establecen las acciones específicas que el sujeto obligado implementará para corregir deficiencias, fortalecer controles y reducir los riesgos identificados, cuya divulgación podría comprometer la seguridad del sistema de tratamiento de datos personales, de conformidad con lo dispuesto en los artículos 103, fracción III, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas y en los artículos 3, fracción IX, y 6, párrafo primero, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, así como en el artículo trigésimo octavo de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas

Sección Clasificada del Documento de Seguridad, apartado del Plan de Trabajo.

Se testa el apartado número 9, que contiene el Plan de Trabajo, en virtud de ser un instrumento de gestión que deriva del análisis de riesgo y del análisis de brecha, en él se establecen las acciones específicas que el sujeto obligado implementará para corregir deficiencias, fortalecer controles y reducir los riesgos identificados, cuya divulgación podría comprometer la seguridad del sistema de tratamiento de datos personales, de conformidad con lo dispuesto en los artículos 103, fracción III, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas y en los artículos 3, fracción IX, y 6, párrafo primero, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, así como en el artículo trigésimo octavo de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas

MECANISMOS DE MONITOREO, REVISIÓN Y MEJORA CONTINUA DE LAS MEDIDAS DE SEGURIDAD

Objetivo

El presente apartado tiene por objeto establecer los mecanismos mediante los cuales el H. Ayuntamiento de Arriaga, Chiapas, supervisará, evaluará y verificará la eficacia de las medidas administrativas, físicas y técnicas implementadas para la protección de los datos personales, con el propósito de garantizar su actualización permanente, fortalecer el Sistema de Gestión de Seguridad de Datos Personales y promover la mejora continua.

El monitoreo constituye un proceso permanente orientado a detectar oportunamente riesgos, vulnerabilidades, incumplimientos y áreas de oportunidad, permitiendo implementar acciones preventivas y correctivas que fortalezcan la protección de los datos personales.

I. Alcance

Los mecanismos previstos en el presente apartado serán aplicables a todas las unidades administrativas que realicen tratamientos de datos personales, independientemente del soporte físico o electrónico en que éstos se encuentren.

La supervisión comprenderá el cumplimiento del presente Documento de Seguridad, la eficacia de las medidas implementadas y la observancia de las disposiciones aplicables en materia de protección de datos personales.

II. Monitoreo permanente

La Unidad de Transparencia, con el apoyo de las unidades administrativas, llevará a cabo actividades permanentes de seguimiento que permitan verificar el adecuado funcionamiento del Sistema de Gestión de Seguridad de Datos Personales.

Entre otras, podrán realizarse las siguientes actividades:

- Verificar el cumplimiento del presente Documento de Seguridad.
- Revisar el Inventario Institucional de Tratamientos de Datos Personales.
- Verificar la actualización de los Avisos de Privacidad.
- Revisar la aplicación de las medidas administrativas, físicas y técnicas.
- Dar seguimiento al Análisis de Riesgos.
- Dar seguimiento al Análisis de Brecha.
- Revisar el Registro de Vulneraciones.
- Verificar el cumplimiento del Plan de Contingencia.
- Revisar los controles de identificación y autenticación.
- Verificar los respaldos de información institucional.
- Revisar los registros de supresión y borrado seguro.
- Dar seguimiento al Programa de Capacitación.
- Verificar el cumplimiento del Plan de Trabajo.

Las actividades de monitoreo deberán documentarse mediante los formatos institucionales correspondientes.

III. Evaluación de la eficacia de las medidas de seguridad

El monitoreo no tendrá únicamente como finalidad verificar la existencia de las medidas de seguridad, sino evaluar su eficacia para proteger los datos personales.

La evaluación considerará, entre otros aspectos:

- La disminución de riesgos identificados.
- La atención oportuna de vulneraciones.
- La efectividad de las medidas administrativas implementadas.
- La eficacia de los controles físicos.
- El funcionamiento de las medidas técnicas.
- La recuperación de información mediante respaldos.
- La atención de incidentes conforme al Plan de Contingencia.
- El cumplimiento de las acciones previstas en el Plan de Trabajo.
- La actualización de los tratamientos de datos personales.
- Los resultados obtenidos durante auditorías, verificaciones y autoevaluaciones.

Cuando la evaluación determine que alguna medida resulta insuficiente o ineficaz, deberán implementarse las acciones preventivas o correctivas necesarias.

IV. Revisión institucional

La revisión del Sistema de Gestión de Seguridad de Datos Personales podrá realizarse:

- De manera programada.
- Como resultado de auditorías internas o externas.
- Derivado de autoevaluaciones.
- Cuando ocurra una vulneración de seguridad.
- Cuando exista una reforma legal.
- Cuando se implementen nuevos tratamientos de datos personales.
- Cuando se incorporen nuevas tecnologías.
- Cuando se modifique la estructura administrativa del Ayuntamiento.
- Cuando así lo determine el Comité de Transparencia.

Cada revisión deberá documentarse y, en su caso, generar las acciones de mejora correspondientes.

V. Indicadores de desempeño

Con la finalidad de medir el funcionamiento del Sistema de Gestión de Seguridad de Datos Personales, se utilizarán los siguientes indicadores institucionales:

Indicador	Método de evaluación	Meta	Evidencia
Documento de Seguridad actualizado	Verificación documental	100 %	Documento vigente
Inventario de Tratamientos actualizado	Revisión del inventario	100 %	Inventario actualizado
Avisos de Privacidad actualizados	Revisión documental	100 %	Avisos vigentes
Análisis de Riesgos actualizado	Verificación documental	100 %	Informe de actualización
Análisis de Brecha actualizado	Verificación documental	100 %	Informe de actualización
Vulneraciones atendidas	Revisión del Registro DS-01	100 %	Registro institucional
Respaldos realizados	Revisión del Registro DS-03	Conforme a la programación	Bitácoras de respaldo
Personal capacitado	Revisión del Registro DS-07	100 % del personal que trate datos personales	Constancias de capacitación
Acciones del Plan de Trabajo cumplidas	Seguimiento del DS-06	100 %	Informe de seguimiento

Los indicadores podrán actualizarse cuando las necesidades institucionales así lo requieran.

VI. Acciones preventivas, correctivas y de mejora

Cuando del monitoreo o de las evaluaciones se detecten incumplimientos, vulnerabilidades o áreas de oportunidad, deberán implementarse acciones encaminadas a fortalecer el Sistema de Gestión de Seguridad de Datos Personales.

Entre otras podrán realizarse las siguientes:

- Actualizar el Documento de Seguridad.
- Fortalecer las medidas administrativas.
- Reforzar las medidas físicas.
- Implementar nuevas medidas técnicas.
- Actualizar el Inventario de Tratamientos.
- Actualizar los Avisos de Privacidad.
- Actualizar el Análisis de Riesgos.
- Actualizar el Análisis de Brecha.
- Reforzar los controles de acceso.
- Capacitar nuevamente al personal involucrado.
- Modificar procedimientos internos.
- Actualizar el Plan de Trabajo.

Las acciones implementadas deberán documentarse y dar lugar al seguimiento correspondiente hasta verificar su cumplimiento.

VII. Informe Anual de Evaluación del Sistema de Gestión de Seguridad de Datos Personales

La Unidad de Transparencia elaborará un Informe Anual de Evaluación con la finalidad de documentar el estado que guarda el Sistema de Gestión de Seguridad de Datos Personales.

El informe contendrá, cuando menos:

- Estado del Documento de Seguridad.
- Resultado de las actividades de monitoreo.
- Resultado de las revisiones efectuadas.
- Actualización del Inventario Institucional.
- Vulneraciones registradas durante el periodo.
- Acciones preventivas y correctivas implementadas.
- Cumplimiento del Plan de Trabajo.
- Cumplimiento del Programa de Capacitación.
- Riesgos detectados.
- Áreas de oportunidad identificadas.
- Recomendaciones de mejora.
- Propuesta de actualización del Documento de Seguridad, cuando resulte procedente.

El Informe Anual podrá presentarse al Comité de Transparencia para su conocimiento y, en su caso, para la emisión de recomendaciones.

VIII. Formato DS-02

CÉDULA DE MONITOREO DE MEDIDAS DE SEGURIDAD

Fecha	Unidad Administrativa	Aspecto revisado	Cumple	No cumple	Hallazgos	Acción correctiva	Responsable	Fecha compromiso	Estatus
			☐	☐					

IX. Matriz Institucional de Seguimiento

Elemento sujeto a revisión	Responsable	Periodicidad	Evidencia	Última revisión
Documento de Seguridad	Unidad de Transparencia	Anual	Documento actualizado	
Inventario de Tratamientos	Unidad de Transparencia y Unidades Administrativas	Permanente	Inventario actualizado	
Avisos de Privacidad	Unidad de Transparencia	Anual o cuando exista modificación	Avisos vigentes	
Análisis de Riesgos	Unidad de Transparencia	Anual	Informe de actualización	
Análisis de Brecha	Unidad de Transparencia	Anual	Informe de actualización	
Registro de Vulneraciones (DS-01)	Unidad de Transparencia	Permanente	Registro institucional	
Registro de Respaldos (DS-03)	Unidades Administrativas	Conforme al programa	Bitácoras de respaldo	
Plan de Contingencia	Unidad de Transparencia	Anual	Informe de revisión	
Programa de Capacitación (DS-07)	Unidad de Transparencia	Anual	Constancias y listas de asistencia	
Plan de Trabajo (DS-06)	Unidad de Transparencia	Semestral	Informe de seguimiento	

X. Revisión y actualización del presente apartado

Los mecanismos de monitoreo deberán revisarse y actualizarse cuando:

- Se modifique la legislación aplicable.
- Se implementen nuevos tratamientos de datos personales.
- Se incorporen nuevas tecnologías.
- Existan observaciones derivadas de auditorías, verificaciones o autoevaluaciones.
- Se identifiquen nuevos riesgos o vulnerabilidades.
- Se modifique la estructura orgánica del Ayuntamiento.
- Se actualice el Documento de Seguridad.

Las modificaciones aprobadas deberán incorporarse al presente Documento de Seguridad y comunicarse a las unidades administrativas para su observancia.

PROGRAMA GENERAL DE CAPACITACIÓN EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES

Objetivo

El presente Programa General de Capacitación tiene por objeto establecer las acciones institucionales destinadas a fortalecer los conocimientos, habilidades y competencias de las personas servidoras públicas del H. Ayuntamiento de Arriaga, Chiapas, que intervienen en el tratamiento de datos personales, con la finalidad de garantizar el cumplimiento de los principios, deberes y obligaciones previstos en la legislación aplicable y fortalecer el Sistema de Gestión de Seguridad de Datos Personales.

La capacitación constituye una medida administrativa de seguridad y un mecanismo permanente de prevención para reducir riesgos derivados del tratamiento inadecuado de datos personales.

I. Alcance

El presente Programa será aplicable a todas las personas servidoras públicas que, en el ejercicio de sus funciones, realicen cualquier tratamiento de datos personales, independientemente de la unidad administrativa de adscripción o del medio físico o electrónico utilizado.

La capacitación comprenderá tanto al personal de nuevo ingreso como al personal en funciones que participe en el tratamiento de datos personales.

II. Objetivos específicos

El Programa General de Capacitación tendrá como objetivos específicos:

- Fortalecer la cultura institucional de protección de datos personales.
- Promover el cumplimiento del presente Documento de Seguridad.
- Capacitar al personal respecto de los principios y deberes en materia de protección de datos personales.
- Difundir las medidas administrativas, físicas y técnicas implementadas por el Ayuntamiento.
- Reducir riesgos derivados de errores humanos.
- Promover el adecuado manejo de expedientes físicos y electrónicos.
- Fortalecer la atención de vulneraciones de seguridad.
- Impulsar la mejora continua del Sistema de Gestión de Seguridad de Datos Personales.

III. Diagnóstico de necesidades de capacitación

La Unidad de Transparencia realizará, cuando resulte necesario, un diagnóstico institucional para identificar las necesidades de capacitación en materia de protección de datos personales.

Para ello podrá considerar, entre otros aspectos:

- Cambios en la legislación aplicable.
- Creación de nuevos tratamientos.
- Resultados de auditorías o autoevaluaciones.
- Vulneraciones registradas.
- Cambios tecnológicos.
- Incorporación de personal de nuevo ingreso.
- Cambios en la estructura administrativa.

Los resultados del diagnóstico servirán como base para elaborar el programa anual de capacitación.

IV. Responsables

Corresponde a la Unidad de Transparencia:

- Elaborar el Programa General de Capacitación.
- Promover la realización de actividades de capacitación.
- Coordinar las acciones con las unidades administrativas.
- Llevar el registro institucional de las capacitaciones impartidas.
- Dar seguimiento al cumplimiento del programa.
- Conservar la evidencia documental correspondiente.

Corresponde a las personas titulares de las unidades administrativas:

- Facilitar la participación del personal.
- Promover la asistencia a las actividades de capacitación.
- Aplicar los conocimientos adquiridos en sus áreas de trabajo.

V. Modalidades de capacitación

Las actividades de capacitación podrán desarrollarse mediante:

- Cursos presenciales.
- Cursos virtuales.
- Talleres.
- Conferencias.
- Seminarios.
- Reuniones de trabajo.
- Materiales informativos.
- Circulares institucionales.
- Actividades de sensibilización.
- Cualquier otro mecanismo que contribuya al fortalecimiento de la cultura de protección de datos personales.

VI. Temática mínima

El Programa podrá comprender, entre otros, los siguientes temas:

- Marco jurídico en materia de protección de datos personales.
- Principios y deberes.
- Derechos ARCO.
- Avisos de Privacidad.
- Inventario de Tratamientos.
- Documento de Seguridad.
- Análisis de Riesgos.
- Gestión de Vulneraciones.
- Medidas administrativas, físicas y técnicas.
- Controles de acceso.
- Respaldos y recuperación.
- Plan de Contingencia.
- Supresión y borrado seguro.
- Responsabilidades de las personas servidoras públicas.
- Mejores prácticas institucionales.

La temática podrá actualizarse cuando existan reformas legales o necesidades institucionales.

VII. Programa anual de capacitación

Actividad	Personal objetivo	Responsable	Periodicidad	Evidencia
Inducción al Documento de Seguridad	Personal de nuevo ingreso	Unidad de Transparencia	Cuando exista ingreso de personal	Lista de asistencia

Curso de Protección de Datos Personales	Personal que trate datos personales	Unidad de Transparencia	Anual	Constancias
Taller de Avisos de Privacidad	Responsables de tratamientos	Unidad de Transparencia	Anual	Memoria fotográfica y lista de asistencia
Capacitación sobre Gestión de Vulneraciones	Titulares de áreas	Unidad de Transparencia	Anual	Constancias
Actualización normativa	Personal relacionado con transparencia y protección de datos	Unidad de Transparencia	Cuando existan reformas	Material de capacitación

VIII. Evaluación de la capacitación

Concluidas las actividades de capacitación, la Unidad de Transparencia podrá evaluar su eficacia mediante:

- Listas de asistencia.
- Constancias de participación.
- Cuestionarios de evaluación.
- Ejercicios prácticos.
- Retroalimentación de las personas participantes.
- Verificación de la aplicación de los conocimientos en las unidades administrativas.

Los resultados obtenidos servirán para mejorar las actividades de capacitación futuras.

IX. Registro institucional de capacitación

La Unidad de Transparencia integrará un registro institucional de las actividades de capacitación realizadas.

FORMATO DS-07

REGISTRO DE CAPACITACIÓN EN PROTECCIÓN DE DATOS PERSONALES

Fecha	Actividad	Unidad Administrativa	Número de asistentes	Instructor	Evidencia	Observaciones

X. Seguimiento y mejora continua

La Unidad de Transparencia dará seguimiento al cumplimiento del presente Programa y promoverá su actualización cuando:

- Existan reformas legales.
- Se incorporen nuevos tratamientos de datos personales.
- Se detecten nuevas necesidades de capacitación.
- Se identifiquen vulneraciones relacionadas con errores humanos.
- Se modifique el Documento de Seguridad.
- Se deriven observaciones de auditorías, verificaciones o autoevaluaciones.

Las modificaciones que resulten necesarias deberán integrarse al Programa General de Capacitación y comunicarse a las unidades administrativas para su implementación.

ÍNDICE

Presentación 2
Objetivo del Documento de Seguridad Municipal 3
Responsabilidades y Atribuciones 3
Alcance del Documento de Seguridad 4
Sistema de Gestión de los Datos Personales 5
Funciones y Obligaciones del Responsable, Encargados y Personas que Traten Datos Personales 8
Resguardo de los Soportes Físicos y/o Electrónicos de los Datos Personales 11
Bitácoras de Acceso, Operación Cotidiana y Vulneraciones a la Seguridad de los Datos Personales 13
Análisis de Brecha 15
Inventario de los Tratamientos y Datos Personales 18
Funciones y Responsabilidades del Tratamiento de Datos Personales 22
Análisis de Riesgos 24
Análisis de la Información 30
Gestión de Vulneraciones a la Seguridad de los Datos Personales 35
Medidas de Seguridad Administrativas, Físicas y Técnicas 38
Controles de Identificación y Autenticación de Usuarios 40
Procedimientos de Respaldo y Recuperación de los Datos Personales 42
Plan de Contingencia 44
Técnicas Utilizadas para la Supresión y Borrado Seguro de los Datos Personales 48
Plan de Trabajo para la Implementación de Medidas de Seguridad 51
Mecanismos de Monitoreo, Revisión y Mejora Continua de las Medidas de Seguridad 53
Programa General de Capacitación en Materia de Protección de Datos Personales 57
Formato DS-07. Registro de Capacitación en Protección de Datos Personales 61