DOCUMENTO DE SEGURIDAD PARA LA PROTECCIÓN DE DATOS PERSONALES

1. Introducción
2. Objetivos y Alcance del Documento
3. Sistema de Gestión de Seguridad de los Datos Personales
4. 4. Inventario De Datos Personales y de Los Sistemas De Tratamiento
5. Funciones y Obligaciones de las Personas que Tratan Datos Personales
6. Análisis de Riesgos y de Brecha
7. Gestión de Vulneraciones y Plan de Contingencia
8. Medidas de Seguridad Generales
   - 8.1. Medidas Administrativas
   - 8.2. Medidas Físicas
   - 8.3. Medidas Técnicas
9. Plan de Trabajo
10. Programa de Capacitación en Protección de Datos Personales

1. INTRODUCCIÓN

La Constitución Política de los Estados Unidos Mexicanos, en sus artículos 6.º, Apartado A, y 16, párrafo segundo, reconoce el derecho fundamental de toda persona a la protección de sus datos personales, así como al ejercicio de los derechos de Acceso, Rectificación, Cancelación y Oposición (ARCO). En su calidad de Sujeto Obligado, el H. Ayuntamiento Municipal Constitucional de Capitán Luis Ángel Vidal, Chiapas, encabezado por la Presidente Municipal C. Emiselda Roblero González, tiene el deber legal y ético de garantizar que el tratamiento de los datos personales resguardados en el ejercicio de sus funciones públicas se realice de manera lícita, segura, leal y confidencial, previniendo cualquier acceso no autorizado, daño, pérdida, alteración o divulgación indebida. Con base en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas y los Lineamientos locales aplicables, el presente Documento de Seguridad establece las políticas, controles y lineamientos organizacionales del Sistema de Gestión de Seguridad institucional.

2. OBJETIVOS Y ALCANCE DEL DOCUMENTO

2.1. Objetivos Generales Establecer y consolidar el conjunto de medidas de seguridad administrativas, físicas y técnicas aplicables en el H. Ayuntamiento de Capitán Luis Ángel Vidal, Chiapas, garantizando la confidencialidad, integridad y disponibilidad de los datos personales bajo su resguardo.

2.2. Objetivos Específicos Identificar formalmente las vulnerabilidades, amenazas y riesgos asociados a los sistemas de tratamiento físicos y digitales del Ayuntamiento. Implementar mecanismos preventivos y correctivos que mitiguen los riesgos en el tratamiento de los datos personales. Definir los protocolos institucionales de respuesta y planes de contingencia ante posibles vulneraciones a la seguridad.

2.3. Alcance del Documento Comprende la totalidad de los tratamientos realizados en soportes físicos y electrónicos por las distintas unidades administrativas del Ayuntamiento de Capitán Luis Ángel Vidal: Presidencia Municipal, Secretaría Municipal, Tesorería, Contraloría, Obras Públicas, Protección Civil, Seguridad Pública y Unidad de Transparencia.

3. SISTEMA DE GESTIÓN DE SEGURIDAD DE LOS DATOS PERSONALES

El Ayuntamiento opera un Sistema de Gestión de Seguridad integral fundado en los principios rectores de la materia: Licitud, Finalidad, Lealtad, Consentimiento, Calidad, Proporcionalidad, Información y Responsabilidad. Este sistema contempla el ciclo completo de vida de los datos personales mediante una estructura secuencial de control:

Datos Personales

Análisis Riesgo

Medidas Control

Análisis Brecha

Mejora Continua

4. INVENTARIO DE DATOS PERSONALES Y DE LOS SISTEMAS DE TRATAMIENTO

Para el debido cumplimiento de las obligaciones es necesario que cada una de las unidades administrativas realice un diagnóstico de los tratamientos de datos personales que llevan a cabo a partir de los siguiente:

Estos tratamientos se realizan en absoluto apego a sus funciones, a través de las diversas áreas que las integran y permiten el desarrollo de los procesos que realizan para el cumplimiento de dichas funciones.

Categoría de Datos	Descripción y Ejemplos de Datos Tratados	Finalidades Generales
Identificación y Contacto	Nombre, firma, domicilio, CURP, RFC, teléfono, correo electrónico, grado académico, fotografía y huella dactilar	Gestión de trámites, atención ciudadana, padrones de beneficiarios, expedientes de personal y registro de accesos
Patrimoniales y Financieros	Cuentas bancarias, CLABE interbancaria, trámites fiscales y pagos patrimoniales.	Contratación de proveedores, pago de nómina, viáticos y subsidios oficiales.
Datos Sensibles	Datos de salud, alergias, antecedentes médicos, discapacidades o condición de vulnerabilidad.	Programas de desarrollo social, atención médica municipal, protección civil y expedientes laborales.
Laborales	Cargo, área de adscripción, correo institucional, teléfono oficial y nombramientos.	Administración de recursos humanos y directorio de servidores públicos

5. FUNCIONES Y OBLIGACIONES DE LAS PERSONAS QUE TRATAN DATOS PERSONALES

1. El H. Ayuntamiento Constitucional: Actúa como Sujeto Obligado responsable del tratamiento general de las bases de datos.

2. Comité de Transparencia: Coordina, dictamina y supervisa las acciones e instrumentos de protección de datos en el municipio.

3. Unidad de Transparencia: Funge como enlace operacional encargado de integrar el Inventario, supervisar Avisos de Privacidad, estructurar el Documento de Seguridad y gestionar solicitudes ARCO.

4. Servidores Públicos Operativos: Toda persona servidora pública que maneje datos personales debe sujetarse estrictamente a las medidas administrativas, físicas y técnicas vigentes, manteniendo el deber ineludible de confidencialidad.

6. ANÁLISIS DE RIESGOS Y DE BRECHA

Sección clasificada del documento de seguridad, apartado análisis de riesgo y brecha. Se testa el apartado número 6 que contiene el análisis de riesgo y brecha, que contiene información que identifica las vulnerabilidades, debilidades, amenazas y deficiencias de las medidas de seguridad implementada por el sujeto obligado

Para su divulgación podría facilitar el acceso no autorizados, vulnerables de datos personales o afectar la eficiencia de los controles de seguridad, de conformidad con los dispuesto en los artículos 103, fracción II, 112 fracción VII, de la ley de transparencia y acceso a la información publica 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 elaboración de versiones publicas

7. GESTIÓN DE VULNERACIONES Y PLAN DE CONTINGENCIA

Sección de clasificada del documento de seguridad, apartado del programa de trabajo para la implementación de medidas de seguridad

Se testa apartado número 7 que contiene el programa de trabajo para la implementación de medidas de seguridad con tiene información que identifica las vulnerabilidades, debilidades amenazas y deficiencias de las medidas de seguridad implementada por el sujeto obligado. su divulgación podría facilitar accesos no autorizados, vulneraciones de datos personales, o afectar la eficiencia de los controles de seguridad.

8. MEDIDAS DE SEGURIDAD GENERALES

8.1. Medidas Administrativas

a) Registro formal de préstamos, altas, bajas y transferencias de expedientes físicos.
b) Políticas de control de acceso a sistemas basadas en el principio de mínimo privilegio.
c) Acuerdos y obligaciones de confidencialidad signados por los servidores públicos. Programas periódicos de capacitación y sensibilización en protección de datos personales.
d) Notificación oportuna ante el Órgano Interno de Control frente a irregularidades o incidentes.

8.2. Medidas Físicas

a) Resguardo de expedientes e impresos en archiveros con cerradura o áreas de acceso restringido.
b) Política de "Escritorios Limpios" e impresoras/escáneres libres de documentos expuestos.
c) Equipos de prevención de incendios (extintores) en áreas de archivo y cómputo.
d) Registro de bitácoras para visitantes a las áreas de resguardo documental.

8.3. Medidas Técnicas

a) Cuentas de usuario individuales con claves de acceso robustas e intransferibles.
b) Respaldos periódicos de la información almacenada en equipos centrales.
c) Antivirus actualizado y controles informáticos administrados por el área correspondiente.
d) Protocolos seguros para la baja, borrado seguro o reasignación de equipos informáticos.

9. PLAN DE TRABAJO

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

10. PROGRAMA DE CAPACITACIÓN EN PROTECCIÓN DE DATOS PERSONALES

La aplicación del programa de protección de datos personales en el H. Ayuntamiento Municipal de Capitán Luis Ángel Vidal, Chiapas; tenemos un objetivo esencial, la formación y sensibilización de las personas que aquí laboran, de tal forma que pueda garantizarse la actualización y mejora continua del inventario de datos personales, la observancia de la normatividad y Ley, por lo que se propone un programa de capacitación en el tema de protección de datos personales que favorezca la profundización en el conocimiento del tema por parte de quienes intervienen en el tratamiento de datos personales.

a) Principios, deberes y obligaciones del marco normativo en datos personales.
b) Elaboración, actualización y difusión adecuada de Avisos de Privacidad.
c) Atención efectiva y oportuna a solicitudes de ejercicio de Derechos ARCO.
d) Prevención de incidentes, seguridad digital y gestión documental adecuada.