PROYECTO DE DOCUMENTO DE SEGURIDAD

HONORABLE JUNTA MUNICIPAL DE CONSTITUCION.

UNIDAD DE TRANSPARENCIA

Documento de Seguridad
De Datos Personales en Posesión de la
Honorable Junta Municipal de
Constitución.

Í N D I C E

I.- OBJETIVO GENERAL

Para la Honorable junta municipal de constitución, en su carácter de sujeto obligado por la Ley de Transparencia y Acceso a la Información Pública del Estado de Campeche; la información es un activo que debe protegerse mediante un conjunto de procesos y sistemas diseñados, administrados y mantenidos permanentemente, de esta manera, la gestión de la seguridad de la información, como parte de un sistema administrativo, busca establecer, implementar, operar y mejorar los procesos y sistemas relativos a la confidencialidad, integridad y disponibilidad de la información personal que permita garantizar la protección de datos personales de los ciudadanos en posesión de este organismo como sujeto obligado.

Teniendo como propósito controlar internamente los sistemas de datos personales que posee, el tipo de datos personales que contiene cada uno, delimitando las obligaciones de cada uno de los responsables, encargados y usuarios de cada sistema y las medidas de seguridad administrativa, física y técnica, que deberán implementarse para el correcto manejo de la información que se posee.

Debiendo mantenerse siempre actualizado, siendo de observancia obligatoria para todos los servidores públicos de la dependencia en cumplimiento a las funciones que les son inherentes; así como para las personas externas que debido a la prestación de algún servicio deba tener acceso a información, sistema o sitio web en el que se ubique cualquier tipo de dato personal protegido por la Honorable Junta Municipal de Constitución.

II.- FUNDAMENTACIÓN JURÍDICA

El presente Documento de Seguridad ha sido elaborado por la Unidad de Transparencia y el Comité de Transparencia de esta Honorable junta municipal de constitución con fundamento en los artículos 1, 44, 45 Fracción III, 72 y 73 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Campeche; en los artículos 1, 2, 3, 4, 5, 6, 7, Capítulo III artículos del 48 al 64, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Campeche; y en el numeral Sexto de los Lineamientos para la Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Campeche.

III.- GLOSARIO

Concepto	Descripción
Áreas Administrativas	Instancias que pertenecen al sujeto obligado que cuenten o puedan contar, dar Tratamiento y ser responsables o encargados, usuarias de los sistemas y bases de datos personales previstos en las disposiciones legales aplicables.
Aviso de Privacidad	Documento físico, electrónico o en cualquier formato generado por el sujeto obligado que es puesto a disposición del titular con el objeto de informarle los Propósitos del tratamiento al que serán sometidos sus datos personales.
Bases de datos	Conjunto ordenado de datos personales referentes a una persona física identificada o identificable, condicionado a criterios determinados con Independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.
Capacitación	Proceso educativo a corto, mediano y largo plazo, que utiliza un procedimiento planeado, sistemático y organizado a través del cual el personal administrativo designado por el sujeto obligado, adquirirá los conocimientos y las habilidades técnicas necesarias para acrecentar su eficacia en la protección de datos Personales.
Comité de Transparencia	Comité de Transparencia del Sujeto Obligado.
Consentimiento	Manifestación de la voluntad libre, específica, informada e inequívoca de la o el titular de los datos personales para aceptar el tratamiento de su información.
Datos personales:	Es la información concerniente a una persona física identificada o identificable, establecida en cualquier formato o modalidad, y que esté almacenada en los sistemas y bases de datos. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier documento informativo físico o electrónico, tales como el nombre, domicilio, números telefónicos, números de seguridad social, relativas al patrimonio, profesión u oficio, características físicas, morales o emocionales, a su vida Afectiva o familiar, entre otros.
Datos personales sensibles	Los datos personales sensibles son aquellos que se refieren a la esfera íntima de su Titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste, tales como los relativos a su origen étnico, o racial, estado de salud, información genética, datos biométricos, creencias

	Religiosas, filosóficas y morales, opiniones políticas o preferencias sexuales uotros similares.
Derechos ARCO	Son los derechos de Acceso, Rectificación, Cancelación y Oposición al tratamiento de datos personales.
Disociación	El procedimiento mediante el cual los datos personales no pueden asociarse al titular ni permitir, por su estructura, contenido o grado de desagregación, la Identificación del mismo.
DNS	Un Servidor DNS en informática responde a las siglas *Domain Name System*. Gracias a los servidores DNS conocemos los nombres en las redes, como las de Internet o las de una red privada.
Documentos	Expedientes, reportes, estudios, actas, dictámenes, resoluciones, oficios, correspondencia, acuerdos, directivas, directrices, circulares, contratos, convenios, instructivos, datos, notas, memorandos, estadísticas, instrumentos de medición o bien, cualquier otro registro que documente el ejercicio de las facultades, funciones, actividad y competencias de los sujetos obligados, sus servidores públicos e integrantes, sin importar su fuente o fecha de elaboración, los cuales podrán estar en cualquier medio, sea escrito, impreso, sonoro, visual, electrónico, informático y holográfico.
Documento de seguridad	Instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales Que posee.
Encargado	Persona física o jurídica, pública o privada, ajena a la organización del responsable, que sola o conjuntamente con otras, trata datos personales a Nombre y por cuenta del responsable.

Evaluación de impacto en la protección de datos personales	Documento mediante el cual se valoran y determinan los impactos reales respecto de determinado tratamiento de datos personales, a efecto de Identificar, prevenir y mitigar posibles riesgos que puedan comprometer el cumplimiento de los principios, deberes, derechos y demás obligaciones.
Expediente	Unidad documental constituida por uno o varios documentos de archivo, Ordenados y relacionados por un mismo asunto, actividad o trámite de los sujetosobligados.
Gestión Administrativa	Forma en que se utilizan los recursos para conseguir los objetivos en materia de protección de datos personales.
INAI	Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.
COTAIPEC	Comisión de Transparencia y Acceso a la Información Pública del Estado de Campeche.
LAN	Una red de área local o LAN (por las siglas en inglés de *Local Área Network*) es una red de computadoras que abarca un área reducida a una casa, un departamento o un edificio.
Ley	Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Campeche.
Ley de Transparencia	Ley de Transparencia y Acceso a la Información Pública del Estado de Campeche.
Ley General	Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
Ley General de Transparencia	Ley General de Transparencia y Acceso a la Información Pública.
Medidas de seguridad	Conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permiten garantizar la protección, confidencialidad, Disponibilidad e integridad de los datos personales.
Medidas de seguridad administrativas	Políticas y procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, la identificación, clasificación y borrado seguro De la información, así como la sensibilización, formación y capacitación del personal en materia de protección de datos personales.
Medidas de seguridad físicas	Conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento.
Medidas de seguridad técnicas	Conjunto de acciones y mecanismos que se valen de la tecnología relacionada con Hardware y software para proteger el entorno digital de los datos personales y recursos involucrados en su tratamiento.
N/A	No aplica.
Plan de Contingencia	Conjunto de procedimientos alternativos a la operatividad normal del sujeto obligado. Su finalidad es la de permitir el funcionamiento de éste, aun cuando

	Alguna de sus funciones deje de hacerlo por algún incidente suscitado, tanto interno como ajeno al organismo.
Portabilidad	Posibilidad de tratar datos personales por vía electrónica en un formato estructurado y comúnmente utilizado, el titular tiene derecho a obtener de los sujetos obligados ante los cuales haya entregado su información una copia de los Datos objeto de tratamiento en el mismo formato que le permita seguir utilizándolos.
Prevención	Medidas precautorias necesarias y adecuadas con la misión de contrarrestar un perjuicio o algún daño que pueda producirse.
Responsable	Los sujetos obligados que determinarán los fines, medios y alcance y demás cuestiones relacionadas con un tratamiento de datos personales.
Sujeto Obligado	Cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, los sindicatos y cualquier persona o jurídica que reciba y ejerza recursos públicos o realice actos de autoridad en el ámbito estatal y municipal serán responsables de los datos personales, sin perjuicio de lo previsto en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Campeche.
Supresión	La baja archivística de los datos personales conforme a la normativa archivística aplicable, que resulte en la eliminación, borrado o destrucción de los datos personales bajo las medidas de seguridad previamente establecidas por el responsable.
Titular	Persona física a quien pertenecen los datos personales.
Transferencia	Toda comunicación de datos personales dentro o fuera del territorio mexicano, realizada a persona distinta del titular, responsable o encargado.
Transparencia	Conjunto de disposiciones y actos mediante los cuales los sujetos obligados tienen el deber de poner a disposición de cualquier persona la información pública que poseen y dar a conocer, en su caso, el proceso y la toma de Decisiones de acuerdo a su competencia, así como las acciones en el ejercicio de sus funciones.
Tratamiento	De manera enunciativa más son limitativa cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionadas con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, Almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación,transferencia o disposición de datos personales.
Unidad de Transparencia	Unidad de Transparencia de la Honorable Junta Municipal de Constitución.
Verificación	Evaluación y valoración regular de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento de datos personales.

Versión Pública	Documento o expediente en el que se da acceso a información eliminando u omitiendo las partes o secciones clasificadas, de conformidad con la Ley General.
Violaciones a la Seguridad	La violación de la seguridad de los datos personales que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transferidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos, o cualquier otra que afecte la confidencialidad, integridad y disponibilidad de los datos personales.

IV. ANTECEDENTES

IV.1. Datos Personales

Los datos personales son cualquier información concerniente a una persona física identificada o identificable y los demás datos sensibles son aquellos datos personales que afecten a la esfera íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste.

En particular, se consideran datos sensibles aquellos que puedan revelar aspectos como origen racial o étnico, estado de salud presente y/o futuro, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas y la preferencia sexual.

Toda persona tiene derecho a la protección de sus datos personales y nadie podrá ser obligado a proporcionar información referente a sus datos sensibles o aquella que pudiera propiciar expresión de discriminación o intolerancia sobre su persona, honor, reputación y dignidad, salvo que la información sea estrictamente necesaria para proteger su vida y seguridad personal o lo prevea alguna disposición, de manera que el catálogo de la información confidencial son los datos personales de una persona física identificada o identificable relativos a origen étnico o racial, características físicas, morales o emocionales, vida afectiva o familiar, domicilio particular, número telefónico y correo electrónico particulares, patrimonio, ideología, opinión política, afiliación sindical y creencia o convicción religiosa y filosófica, estado de salud mental e historial médico, preferencia sexual y otras análogas que afecten su intimidad, que puedan dar origen a discriminación o que su difusión o entrega a terceros conlleve un riesgo para su titular, la entregada con tal carácter por los particulares, siempre que: se precisen los medios en que se contiene y no se lesionen derechos de terceros o se contravengan disposiciones de orden público, además de la considerada como confidencial por disposición legal expresa.

Por consiguiente, los datos personales se clasificarán de manera enunciativa, más no limitativa de acuerdo con las siguientes características:

1. **Identificativos:** El nombre, domicilio, teléfono particular, teléfono celular, firma, clave de Registro Federal de Contribuyentes (RFC), Clave Única de Registro de Población (CURP), Clave de Elector, Matricula del Servicio Militar Nacional, número de pasaporte, lugar y fecha de nacimiento, nacionalidad, edad, fotografía y demás análogos.

2. **Datos de origen:** Documentos que contengan datos referentes al origen étnico o racial.
3. **Datos ideológicos:** Son aquellos referentes a la ideología u opinión política, opinión pública, afiliación sindical y creencia o convicción religiosa o filosófica.
4. **Datos de salud:** El expediente clínico de cualquier atención médica, referencias o descripción de sintomatologías, detección de enfermedades, incapacidades médicas, discapacidades, intervenciones quirúrgicas, vacunas, consumo de estupefacientes, uso de aparatos oftalmológicos, ortopédicos, auditivos, prótesis, estado físico o mental de la persona, así como la información de la vida sexual.
5. **Datos laborales:** Documentos de reclutamiento y selección, nombramiento, incidencia, capacitación, actividades extracurriculares, referencias laborales, referencias personales, solicitud de empleo, hoja de servicios y demás análogos.
6. **Datos patrimoniales:** De bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos y egresos, cuentas bancarias, seguros, fianzas, servicios contratados, referencias personales y demás análogas.
7. **Datos sobre procedimientos administrativos y/o jurisdiccionales:** La información relativa a una persona que se encuentre sujeta a un procedimiento administrativo en forma de juicio jurisdiccional en materia laboral, civil, penal, fiscal, administrativa, o de cualquier otra rama del derecho.
8. **Datos académicos:** Trayectoria educativa, calificaciones, títulos, cédula profesional, certificados y reconocimientos y demás análogos.
9. **Datos de tránsito y movimientos migratorios:** Información relativa al tránsito de las personas dentro y fuera del país, así como información migratoria.

Los datos personales solo pueden ser transferidos a terceros, en los casos previstos en el artículo 101 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Campeche, las cuales establecen que no se requiere autorización del titular de la información confidencial para proporcionarla a terceros en los supuestos allí establecidos.

En el caso de la transferencia de información protegida, el responsable de dicha información deberá asegurarse que cuente al menos medidas de protección como: la carátula al inicio del documento, con la leyenda relativa al tipo de información que contenga, nombre y cargo del destinatario, en caso de tratarse de un documento electrónico deberá remitirse en un formato de archivo que no permita su edición o manipulación y deberá estar protegido de origen contra impresión y copiado no autorizado, parcial o total, de su contenido, utilizando mecanismos que aseguren la información únicamente será tratada por el destinatario autorizado a recibirla, comunicar sobre la responsabilidad que éstos adquieren al recibir la información a que se refiere el artículo 101 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Campeche, contenerse en sobre cerrado y sellado, cuyo traslado será a cargo de servidores públicos del sujeto obligado autorizado para ello, además de las medidas de protección que, de acuerdo a los riesgos y amenazas, el sujeto obligado considere necesario adoptar.

De manera que los titulares de la información confidencial tienen los siguientes derechos: tener libre acceso a la información confidencial que posean los sujetos obligados, conocer la utilización, procesos modificaciones y transmisiones de que sea objeto su información confidencial, solicitar la rectificación, modificación, corrección, sustitución, oposición, supresión o ampliación de datos de información confidencial, autorizar por escrito ante dos testigos o mediante escritura pública, la difusión, distribución, publicación, transferencia o comercialización de su información confidencial, además de las que establezcan las disposiciones legales.

En consecuencia, cuando el titular de la información confidencial fallezca o sea declarada judicialmente su presunción de muerte, los derechos reconocidos en esta ley respecto a su información confidencial pasarán sin ningún trámite a sus familiares cercanos, primero en línea recta sin limitación de grado y, en su caso, a los colaterales hasta el cuarto grado, en caso de conflictos familiares con igual parentesco por la titularidad de los derechos, lo resolverá la autoridad competente.

Si los ciudadanos o instituciones privadas, proporcionan a la Honorable Junta Municipal De Constitución, información confidencial, se les dará a conocer las políticas respecto a su protección, de conformidad con los lineamientos que establezca la Comisión de Transparencia y Acceso a la Información Pública del Estado de Campeche, a su vez tomará medidas necesarias que garanticen la seguridad de dicha información y eviten su alteración, pérdida, transmisión, publicación y acceso no autorizado.

IV.2. Derecho ARCO

En la Constitución Política de los Estados Unidos Mexicanos se establece que, toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la Ley, la cual establecerá los supuestos de excepción a los principios que rigen el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros.

Por ende, la persona que sea titular de la información de carácter confidencial que se encuentre en posesión de la Honorable Junta Municipal de Constitución, puede solicitar en cualquier tiempo su acceso, clasificación, rectificación, oposición, modificación, corrección, sustitución, cancelación o ampliación de datos, sin embargo no es aplicable cuando exista un procedimiento especial en otras disposiciones legales.

La solicitud de acceso, rectificación o supresión de datos personales, podrá realizarse solamente por el titular de la misma o su representante legal, por razones de seguridad y protección de datos personales, requiere presentar identificación oficial con fotografía tanto para solicitar como para recibir esta información.

La cancelación de datos personales dará lugar a un período de bloqueo tras el cual se procederá a la supresión del dato.

El sujeto obligado podrá conservarlos exclusivamente para efectos de responsabilidades nacidas del tratamiento y el periodo de bloqueo será equivalente al plazo de prescripción de acciones derivadas de la relación jurídica que funda el tratamiento en los términos de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Campeche.

Una vez cancelado el dato por parte del sujeto obligado, éste dará aviso a su titular dentro de los cinco días hábiles siguientes, por consiguiente cuando los datos personales hubiesen sido transmitidos con anterioridad a la fecha de rectificación o cancelación y sigan siendo tratados por terceros, el sujeto obligado deberá hacer de su conocimiento dicha solicitud de rectificación o cancelación, para que proceda a efectuarla, tal como lo establece la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Campeche.

Una vez recibida la solicitud de acceso, rectificación o supresión de datos personales, se deberá verificar que se haga en términos respetuosos y tenga el nombre del sujeto obligado a quien se dirige, el nombre del solicitante titular de la información y del representante legal, el domicilio, número de fax o correo electrónico para recibir notificaciones y el planteamiento concreto sobre el acceso, clasificación, rectificación, oposición, modificación, corrección, sustitución, cancelación, o ampliación de datos que solicita, además de acompañar copia simple de los documentos en los que se apoye su solicitud, de conformidad a lo establecido en el artículo 78 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Campeche.

Reconociendo que el ejercicio de las atribuciones de las dependencias y entidades de la Administración Pública implica recabar datos personales para los fines establecidos en las disposiciones aplicables, por lo que los servidores públicos deben ser los primeros obligados al cumplimiento de la Ley para promover el uso responsable de las nuevas tecnologías de la información, atendiendo los principios de protección de datos personales de licitud, calidad de la información, de seguridad, custodia y consentimiento para su transmisión; principios que no limitan la utilización de la informática en el ámbito público, sino que se trata de hacerla compatible con los derechos de los ciudadanos.

Será confirmación confidencial cuando se trate de una persona física, identificada o identificable, debiendo entenderse como identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, y que en razón de su contenido permita acceder al conocimiento de diversos aspectos de la persona, incluso obtener una imagen diversificada y compleja de la misma, apta para establecer perfiles de categorización a través de múltiples operaciones de tratamiento a que puedan ser sometidas, que puedan vincularse entre sí, afectando los datos más frágiles y vulnerables de la esfera del ser humano, a través de la exhibición pública y de la incursión sin consentimiento previo a la vida íntima y familiar de la persona.

IV.3. Tratamiento de la Información por parte de los Sujetos Obligados

Los sujetos obligados deberán adoptar medidas necesarias para el manejo, mantenimiento, seguridad y protección de la información confidencial que obre en su poder, así como los procedimientos para garantizar la protección, tratamiento, mantenimiento y seguridad de los datos personales que posean con motivo de sus atribuciones.

Para el tratamiento de datos personales, los sujetos obligados deberán observar los principios de licitud, confidencialidad, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, así como las medidas necesarias para el manejo, mantenimiento, seguridad y protección a cabalidad de dicha información.

La licitud es toda aquella recolección de datos personales que se realiza a través de los medios legales o reglamentarios de cada sujeto obligado previsto para tales efectos; la confidencialidad se refiere a garantizar que exclusivamente la persona interesada pueda acceder a sus datos personales o, en su caso, el responsable o el usuario del sistema de información confidencial para su tratamiento a la par de terceros responsables los cuales tienen el deber de la secrecía; el principio de consentimiento es la manifestación de voluntad libre, inequívoca, especifica e informada, mediante el cual el interesado consiente el tratamiento de sus datos personales; el principio de información consiste en hacer del conocimiento del titular de los datos, al momento de recabarlos y de forma escrita, el fundamento y motivo de ello, así como finalidades y usos para los cuales se tratará dicha información; por el principio de calidad se deberá entender que el tratamiento deberá ser exacto, adecuado y pertinente.

IV.4. Medidas de seguridad implementadas

En la Honorable Junta Municipal de Constitución, conjuntamente con las áreas administrativas responsables de los sistemas de tratamiento de datos personales y con el área encargada de las tecnologías de la información, adopta todas aquellas medidas necesarias para la protección de datos personales y así asegurar que la información confidencial que posee sea resguardada, de manera íntegra, segura yadecuada a través de sus políticas de procesos, controles, mecanismos administrativos, físicos y técnicos implementados. Los tipos de medidas de seguridad a implementarse son **administrativa, física y técnica.**

a) Las medidas de seguridad administrativa son aquellas que deben implementarse para la consecución de los objetivos contemplados en los siguientes apartados:

- **Política de seguridad.** Definición de directrices estratégicas en materia de seguridad de activos, alineadas a las atribuciones de las dependencias o entidades. Incluye la elaboración y emisión interna de políticas, entre otros documentos regulatorios del sujeto obligado.
- **Cumplimiento de la normatividad.** Los controles establecidos para evitar violaciones de la normatividad vigente, obligaciones contractuales o la política de seguridad interna. Abarca, entre otros, la identificación y el cumplimiento de requerimientos tales como la legislación aplicable.
- **Organización de la seguridad de la información.** Establecimiento de controles internos y externos a través de los cuales se gestione la seguridad de activos. Considera, entre otros aspectos, la organización interna, que a su vez se refiere al compromiso de la alta dirección y la designación de responsables, entre otros objetivos; asimismo, considera aspectos externos como la identificación de riesgos relacionados con terceros.
- **Clasificación y control de activos.** Establecimiento de controles en materia de identificación, inventario, clasificación y valuación de activos conforme a la normatividad aplicable.
- **Seguridad relacionada a los recursos humanos.** Controles orientados a que el personal conozca el alcance de sus responsabilidades respecto a la seguridad de activos, antes, durante y al finalizar la relación laboral.
- **Administración de incidentes.** Implementación de controles enfocados a la gestión de incidentes presentes y futuros que puedan afectar la integridad, confidencialidad y disponibilidad de la información. Incluye temas como el reporte de eventos y debilidades de seguridad de la información.
- **Continuidad de las operaciones.** Establecimiento de medidas con el fin de contrarrestar las interrupciones graves de la operación y fallas mayores en los sistemas de información. Incluye planeación, implementación, prueba y mejora del plan de continuidad de la operación del sujeto obligado.

b) Las medidas de seguridad física atañen a las acciones que deben implementarse para contar con:

- **Seguridad física y ambiental.** Establecimiento de controles relacionados con los perímetros de seguridad física y el entorno ambiental de los activos, con el fin de prevenir accesos no autorizados, daños, robo, entre otras amenazas. Se enfoca en aspectos tales como los controles implementados para espacios seguros y seguridad del equipo.

c) Las medidas de seguridad técnica son las aplicables a sistemas de datos personales en soportes electrónicos, servicios e infraestructura de telecomunicaciones y tecnologías de la información, entre otras, se prevén las siguientes acciones:

- **Gestión de comunicaciones y operaciones.** Establecimiento de controles orientados a definir la operación correcta y segura de los medios de procesamiento de información, tanto para la gestión interna como la que se lleva a cabo con terceros. Incluye, entre otros aspectos, protección contra código malicioso y móvil, copias de seguridad, gestión de la seguridad de redes y manejo de medios de almacenamiento.

- **Control de acceso.** Establecimiento de medidas para controlar el acceso a la información, activos e instalaciones por parte de los responsables autorizados para tal fin, considerando en ello, la protección contra la divulgación no autorizada de información. Abarca, entre otros temas, gestión de acceso de los usuarios, control de acceso a redes, control de acceso a sistemas operativos y control de acceso a las aplicaciones y a la información.
- **Adquisición, desarrollo, uso y mantenimiento de sistemas de información.** Integración de controles de seguridad a los sistemas de información, desde su adquisición o desarrollo, durante su uso y mantenimiento, hasta su cancelación o baja definitiva. Considera procesamiento adecuado en las aplicaciones, controles criptográficos y seguridad de los archivos de sistema, entre otros.

Tipo de soportes: Es importante explicar la diferencia entre un soporte físico y un soporte electrónico, debido a que las medidas de seguridad que el sujeto obligado implemente para cada sistema de datos personales está estrechamente relacionadas con el tipo de soportes utilizados. Para lograr lo anterior, es preciso referirse a las definiciones que se prevén en las Recomendaciones emitidas por el INAI:

- **Soportes físicos**. Son los medios de almacenamiento inteligibles a simple vista, es decir, que no requieren de ningún aparato que procese su contenido para examinar, modificar o almacenar los datos; es decir, documentos, oficios, formularios impresos llenados "a mano" o "a máquina", fotografías, placas radiológicas, carpetas, expedientes, entre otros.

- **Soportes electrónicos.** Son los medios de almacenamiento inteligibles sólo mediante el uso de algún aparato con circuitos electrónicos que procese su contenido para examinar, modificar o almacenar los datos; es decir, cintas magnéticas de audio, vídeo y datos, fichas de microfilm, discos ópticos (CDS y DVDs), discos magneto-ópticos, discos magnéticos (flexibles y duros) y demás medios de almacenamiento masivo no volátil.

Los lineamientos hacen mención de los conceptos arriba señalados cuando se alude a los tipos de soportes, medios de almacenamiento o formatos: físicos o electrónicos, en los cuales residen los datos personales del sistema que custodia el sujeto obligado. Una vez explicado lo anterior, es preciso señalar que el sujeto obligado deberá identificar el tipo de soporte en el que residen los datos personales de cada uno de los sistemas que posee con el propósito de corroborar que las medidas de seguridad implementadas sean aplicables a cada caso. Por tanto, en el Documento de seguridad deberá constar si los datos personales del sistema residen en:

a) Soporte físico;
b) Soporte electrónico; o
c) Ambos tipos de soportes.

V. DE LOS SISTEMAS DE TRATAMIENTO

Se diseñaron los siguientes sistemas de tratamiento:

SISTEMA DE TRATAMIENTO DE LOS DATOS PERSONALES EN LAS SOLICITUDES PARA EL EJERCICIO DE LOS DERECHOS ARCO		
Nombre del Administrador:	**DANIEL CORIA DAMIAN**	Base de Datos 1. Solicitudes recibidas
Cargo:	**Responsable de la Unidad de Transparencia**	
Área:	**Transparencia**	
Funciones y Obligaciones:	1. Administrar el sistema del sujeto obligado que opere la información fundamental; 2. Actualizar trimestralmente la información fundamental del sujeto obligado; 3. Recibir y dar respuesta a las solicitudes para el ejercicio de los derechos arco, para lo cual debe integrar el expediente, realizar los trámites internos y desahogar el procedimiento respectivo; 4. Llevar el registro y estadística de las solicitudes de información pública. 5. Asesorar gratuitamente a los solicitantes en los trámites para acceder o elaborar una solicitud de información pública; 6. Solicitar al Comité de Transparencia interpretación o modificación de la clasificación de información pública solicitada; y 7. Las demás que establezcan otras disposiciones legales o reglamentarias aplicables.	
Personal autorizado para tratamiento		
Nombre:	**CARLOS MARQUEZ SANTIAGO**	Base de Datos 1. Solicitudes recibidas
Cargo:	**SECRETARIO**	
Área:	**SECRETARIA**	
Funciones y obligaciones:	1. Coadyuvar en la administración del sistema del sujeto obligado que opere la información fundamental; 2. Coordinar la actualización mensual de la información fundamental del sujeto obligado; 3. Apoyar en la recepción y contestación a las solicitudes para el ejercicio de los derechos arco; 4. Asesorar gratuitamente a los solicitantes en los trámites para acceder o elaborar una solicitud de información pública; y 5. Las demás que establezcan otras disposiciones legales o reglamentarias aplicables.	
Personal autorizado para tratamiento		
Nombre:	**OLIVIO DAMAS INURRETA**	Base de Datos 1. Solicitudes recibidas
Cargo:	**TESORERO**	
Área:	**Administración y Finanzas**	
Funciones y Obligaciones:	1. Realizar y auxiliar en la administración del sistema del sujeto obligado que opere la información fundamental; 2. Realizar el soporte electrónico de la información; 3. Coadyuvar en la actualización mensualmente de la información fundamental del sujeto obligado; 4. Auxiliar en el registro y estadística de las solicitudes para el ejercicio de los derechos arco y ; 5. Las de más que establezcan otras disposiciones legales o reglamentarias aplicables.	

Personal autorizado para tratamiento		
Nombre:	**Sandra Isaura Hernández Santiago**	Base de Datos 1. Solicitudes recibidas
Cargo:	**Jurídico**	
Área:	**Área Jurídica**	
Funciones y obligaciones:	1. Coadyuvar en la administración del sistema del sujeto obligado que opere la información fundamental; 2. Coordinar la actualización mensual de la información fundamental del sujeto obligado; 3. Apoyar en la recepción y contestación a las solicitudes para el ejercicio de los derechos arco; 4. Asesorar gratuitamente a los solicitantes en los trámites para acceder o elaborar una solicitud de información pública; y 5. Las demás que establezcan otras disposiciones legales o reglamentarias aplicables.	
Personal autorizado para tratamiento		
Nombre:	**Moisés Hernández Álvarez**	Base de Datos 1. Solicitudes recibidas
Cargo:	**Encargado De Catastro**	
Área:	**Área de Catastro**	
Funciones y Obligaciones:	1. Realizar y auxiliar en la administración del sistema del sujeto obligado que opere la información fundamental; 2. Apoyar en la recepción y contestación a las solicitudes para el ejercicio de los derechos arco. 3. Coadyuvar en la actualización mensualmente de la información fundamental del sujeto obligado; 4. Las demás que establezcan otras disposiciones legales o reglamentarias aplicables.	

TIPO DE DATOS PERSONALES PERTENECIENTES AL SISTEMA DE TRATAMIENTO	
Inventario:	1. Nombre; 2. Correo electrónico 3. Teléfono
Bases de datos:	Solicitudes Recibidas
No. de Titulares:	N/A
Controles de seguridad para las bases de datos	Nombres de usuarios y claves personales de acceso al sistema
ESTRUCTURA Y DESCRIPCIÓN DEL SISTEMA DE TRATAMIENTO	
Tipo de soporte:	Soporte físico y electrónico
Características del lugar de resguardo:	Para acceder a la información se requiere autorización del Titular Equipo de cómputo personal
Programas en que se utilizan los D.P.	Excel, Word, indetec, infomex, Plataforma Nacional de Transparencia y correo electrónico
RESGUARDO DE LOS SOPORTES FÍSICOS Y/O ELECTRÓNICOS EN QUE SE ENCUENTRAN LOS DATOS PERSONALES	

Físicos:	Archivo de documentos bajo llave En lugar adecuado y sin riesgo de contingencias ambientales		
Electrónicos:	Nombres de usuarios y claves personales de acceso al sistema Resguardo de información en disco duro externo		
LAS BITÁCORAS DE ACCESO Y OPERACIÓN COTIDIANA			
Bitácoras Físicas:	N/A		
Clave de la bitácora:	N/A		
Bitácoras Electrónicas:	N/A		
Clave de la bitácora:	N/A		
LAS BITÁCORAS DE VULNERACIONES DE SEGURIDAD			
ID		**Soporte**	**Responsable**
Bitácora de Solicitudes derecho ARCO:	01	Físico, Excel y Word	Unidad de Transparencia

SISTEMA DE TRATAMIENTO DE LOS DATOS PERSONALES EN LAS SOLICITUDES DE ACCESO A LA INFORMACIÓN		
Nombre del Administrador:	**Daniel Coria Damián**	Base de Datos 1. Solicitudes recibidas
Cargo:	**Responsable de la Unidad de Transparencia**	
Área:	**Unidad de Transparencia**	

Funciones y Obligaciones:	1. Administrar el sistema del sujeto obligado que opere la información fundamental; 2. Actualizar trimestralmente la información fundamental del sujeto obligado; 3. Recibir y dar respuesta a las solicitudes de información pública, para lo cual debe integrar el expediente, realizar los trámites internos y desahogar el procedimiento respectivo; 4. Llevar el registro y estadística de las solicitudes de información pública. 5. Asesorar gratuitamente a los solicitantes en los trámites para acceder o elaborar una solicitud de información pública; 6. Solicitar al Comité de Transparencia interpretación o modificación de la clasificación de información pública solicitada; y 7. Las demás que establezcan otras disposiciones legales o reglamentarias aplicables.	
Personal autorizado para tratamiento		
Nombre:	**Sandra Isaura Hernández Santiago**	Base de Datos 1. Solicitudes recibidas
Cargo:	**Jurídico**	
Área:	**Área Jurídica**	
Funciones y obligaciones:	6. Coadyuvar en la administración del sistema del sujeto obligado que opere la información fundamental; 7. Coordinar la actualización mensual de la información fundamental del sujeto obligado; 8. Apoyar en la recepción y contestación a las solicitudes de información pública; 9. Asesorar gratuitamente a los solicitantes en los trámites para acceder o elaborar una solicitud de información pública; y 10. Las demás que establezcan otras disposiciones legales o reglamentarias aplicables.	
Personal autorizado para tratamiento		

Nombre:	**Moisés Hernández Álvarez**	Base de Datos 1. Solicitudes recibidas
Cargo:	**Encargado De Catastro**	
Área:	**Área de Catastro**	
Funciones y Obligaciones:	5. Realizar y auxiliar en la administración del sistema del sujeto obligado que opere la información fundamental; 6. Apoyar en la recepción y contestación a las solicitudes de información pública. 7. Coadyuvar en la actualización mensualmente de la información fundamental del sujeto obligado; 8. Las demás que establezcan otras disposiciones legales o reglamentarias aplicables.	
Personal autorizado para tratamiento		
Nombre:	**CARLOS MARQUEZ SANTIAGO**	Base de Datos 1. Solicitudes recibidas
Cargo:	SECRETARIO	
Área:	SECRETARIA	
Funciones y obligaciones:	1. Coadyuvar en la administración del sistema del sujeto obligado que pere la información fundamental; 2. Coordinar la actualización mensual de la información fundamental del sujeto obligado; 4. Apoyar en la recepción y contestación a las solicitudes de información pública; 5. Asesorar gratuitamente a los solicitantes en los trámites para acceder o elaborar una solicitud de información pública; y 6. Las demás que establezcan otras disposiciones legales o reglamentarias aplicables.	
Personal autorizado para tratamiento		
Nombre:	**OLIVIO DAMAS INURRETA**	Base de Datos 1. Solicitudes recibidas
Cargo:	**TESORERO**	
Área:	**Administración y Finanzas**	
Funciones y Obligaciones:	1. Realizar y auxiliar en la administración del sistema del sujeto obligado que opere la información fundamental; 2.Realizar el soporte electrónico de la información; 3.Coadyuvar en la actualización mensualmente de la información fundamental del sujeto obligado; 4. Auxiliar en el registro y estadística de las solicitudes de información pública; y 5. Apoyar en la recepción y contestación a las solicitudes de información publica 6. Las demás que establezcan otras disposiciones legales o reglamentarias aplicables.	

VI.- DE LAS FUNCIONES Y OBLIGACIONES DE LAS PERSONAS QUE TRATAN DATOS PERSONALES

Para garantizar la aplicación correcta de este sistema es necesario establecer los deberes de los servidores públicos de la Honorable Junta Municipal de Constitución que participan en el tratamiento de los datos personales derivado de sus atribuciones.

Al momento de recibir los datos personales **el servidor público que se encargue de su recepción** deberá:

1. Tener a la vista el Aviso de Privacidad.
2. Dar a conocer el aviso de privacidad al titular de los datos personales previo a la obtención de sus datos.
3. En caso de dudas o quejas de los titulares de los datos personales sobre el tratamiento de sus datos, orientar al ciudadano para que acuda a la Unidad de Transparencia de la Honorable Junta Municipal de Constitución.
4. Al obtener los datos personales cerciorarse de que la información esté completa, actualizada, sea veraz, y comprensible.
5. Comunicar discrepancias de los datos personales recabados a su jefe inmediato o al administrador de los datos personales, ello cuando se dé cuenta.
6. Conocer y seguir las medidas de seguridad que le sean aplicables para el cuidado de los datos personales, durante el periodo en el que posea los datos personales.
7. Recabar los datos personales para la finalidad para la cual estos fueron recabados según el trámite o el sistema de tratamiento que corresponda.
8. Tratar los datos personales de manera lícita siguiendo los principios establecidos en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Campeche.
9. Conocer, aplicar y sujetarse al Aviso de Privacidad y al Documento de Seguridad de la Honorable Junta Municipal de Constitución, en el tratamiento de datos personales.
10. Guardar estricta confidencialidad de los datos personales que conozca en el ejercicio de sus funciones.
11. Tomar, una vez al año un curso, taller o capacitación sobre el tratamiento de datos personales.
12. Sujetarse a lo establecido en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Campeche.

El servidor público involucrado en el tratamiento de datos personales deberá:

1. Conocer, aplicar y sujetarse al Aviso de Privacidad y al Documento de Seguridad de la Honorable Junta Municipal de Constitución, en el tratamiento de datos personales.
2. Aplicar las medidas de seguridad correspondientes a los datos personales tratados y/o el sistema de protección en el que participa.
3. Tratar los datos personales de manera lícita siguiendo los principios establecidos en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Campeche.

4. En caso de dudas o quejas de los titulares de los datos personales sobre el tratamiento de sus datos, orientar al ciudadano para que acuda a la Unidad de Transparencia de la Honorable Junta Municipal de Constitución.

5. Guardar estricta confidencialidad de los datos personales que conozca en el ejercicio de sus funciones.

6. Abstenerse de realizar transferencias de datos personales que no vayan de conformidad con la finalidad para la cual se obtuvieron los datos.

7. Sujetarse a lo establecido en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Campeche.

El servidor público que administra los datos personales, conforme los sistemas de tratamiento vigentes deberá:

1. Conocer, aplicar y sujetarse al Aviso de Privacidad y al Documento de Seguridad de la Honorable Junta Municipal de Constitución, en el tratamiento de datos personales.

2. Conocer e implementar las medidas de seguridad establecidas en el documento de seguridad.

3. Aplicar nuevas medidas de seguridad que resulten accesibles y viables para la protección de datos personales.

4. Supervisar a los servidores públicos que participan en la recepción y en el tratamiento de datos personales en cada trámite o sistema.

5. Tratar los datos personales para la finalidad para la cual estos fueron recabados según el trámite o el sistema de tratamiento que corresponda.

6. Tratar los datos personales de manera lícita siguiendo los principios establecidos en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Campeche.

7. Guardar estricta confidencialidad de los datos personales que conozca en el ejercicio de sus funciones.

8. Tomar, una vez al año, un curso, taller o capacitación sobre el tratamiento de datos personales.

9. Informar a los titulares de los datos sobre nuevas finalidades del tratamiento de datos personales o nuevas transferencias.

10. En caso de dudas o quejas de los titulares de los datos personales sobre el tratamiento de sus datos, orientar al ciudadano para que acuda a la Unidad de Transparencia del Honorable Junta Municipal de Constitución.

11. Informar a la Unidad de Transparencia de la Honorable Junta Municipal de Constitución sobre los cambios que sufran sus trámites o sistemas de tratamiento de datos personales, los riesgos y las vulneraciones que surjan en el tratamiento de los datos personales, las medidas correctivas implementadas y las transferencias nuevas que realicen de los datos personales.

12. Acudir a la Unidad de Transparencia de la Honorable Junta Municipal de Constitución en caso de asesoría sobre el tratamiento de datos personales.

13. Monitorear de manera cotidiana la implementación de las medidas de seguridad y levantar actas circunstanciadas de hechos ante la reincidencia de un incumplimiento en la aplicación de estas.

14. Dar aviso al Comité de Transparencia, a través de la Unidad de Transparencia de la Honorable Junta Municipal de Constitución, sobre las actas circunstanciadas de hechos levantadas por el incumplimiento del documento de seguridad y sobre el seguimiento de estas.

15. Sujetarse a lo establecido en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Campeche.

El servidor público responsable de cada sistema, o en su caso, el **titular de la Unidad Administrativa responsable de cada sistema deberá:**

1. Conocer, aplicar y sujetarse al Aviso de Privacidad y al Documento de Seguridad de la Honorable Junta Municipal de Constitución, en el tratamiento de datos personales.

2. Implementar las medidas de seguridad que establece el documento de seguridad.

3. Guardar estricta confidencialidad de los datos personales que conozca en el ejercicio de sus funciones.

4. Tomar una vez al año un curso, taller o capacitación sobre el tratamiento de datos personales.

5. En caso de dudas o quejas de los titulares de los datos personales sobre el tratamiento de sus datos, orientar al ciudadano para que acuda a la Unidad de Transparencia de la Honorable Junta Municipal de Constitución.

6. Aplicar medidas correctivas en caso de identificar incidentes, alteraciones o vulneraciones en el tratamiento de datos personales.

7. Informar a la Unidad de Transparencia de la Honorable Junta Municipal de Constitución sobre los cambios que sufran sus trámites o sistemas de tratamiento de datos personales, los riesgos y las vulneraciones que surjan en el tratamiento de los datos personales, las medidas correctivas implementadas y las transferencias nuevas que realicen de los datos personales.

8. Monitorear la implementación de las medidas de seguridad.

9. Monitorear de manera cotidiana la implementación de las medidas de seguridad y levantar actas circunstanciadas de hechos ante la reincidencia de un incumplimiento en la aplicación de las mismas.

10. Dar aviso al Comité de Transparencia, a través de la Unidad de Transparencia de la Honorable Junta Municipal de Constitución, sobre las actas circunstanciadas de hechos, levantadas por el incumplimiento del documento de seguridad y sobre el seguimiento de las mismas.

11. Presentar propuestas de mejora o modificación del documento de seguridad a través de la Unidad de Transparencia de la Honorable Junta Municipal de Constitución.

12. Emitir reportes en relación con el tratamiento de los datos personales y la aplicación de medidas de seguridad, según sea requerido por el Comité de Transparencia a través de la Unidad de Transparencia de la Honorable Junta Municipal de Constitución.

13. Diseñar, desarrollar e implementar políticas públicas, procesos internos, y/o sistemas o plataformas tecnológicas necesarias para el ejercicio de sus funciones apegándose en todo momento al documento de seguridad, las políticas o lineamientos que para el tratamiento de datos personales que emita el Comité de Transparencia, la Unidad de Transparencia de la Honorable Junta Municipal de Constitución, así como a la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado Campeche.

14. Sujetarse a lo establecido en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Campeche.

Son obligaciones de la **Unidad de Transparencia** en relación con el tratamiento de datos personales, además de las previstas en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Campeche:

1. Difundir al interior de la Honorable Junta Municipal de Constitución el aviso de privacidad y el documento de seguridad.

2. Proponer al Comité de Transparencia actualizaciones o modificaciones al documento de seguridad.

3. Emitir un reporte anual al Comité de Transparencia sobre el ejercicio de estas funciones.

Son obligaciones del **Comité de Transparencia** en relación con el tratamiento de datos personales, además de las previstas la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Campeche:

1. Revisar anualmente las políticas y/o lineamientos en materia de protección de datos personales establecidos en el presente documento.

2. Emitir o aprobar anualmente un programa de capacitaciones en materia de protección de datos personales.

3. Requerir anualmente a las dependencias o áreas responsables que tratan datos personales, a través de la Unidad de Transparencia de la Honorable Junta Municipal de Constitución, informes sobreel tratamiento de los datos personales y la aplicación de medidas de seguridad, así como vulneraciones detectadas en el año.

VII. DEL ANÁLISIS DE RIESGOS

Debido a las circunstancias generales, tanto físicas como humanas, en las que se tratan datos personales, hemos logrado identificar los siguientes riesgos posibles ante los que se pudiera enfrentar este Sujeto Obligado:

- Obtención de datos incompletos o incorrectos.
- Omitir la notificación al titular de los datos personales del aviso de privacidad.
- No difundir el aviso de privacidad.
- Ante la necesidad de tener un consentimiento expreso: no tener evidencia de que el titular de los datos personales conoce los términos del aviso de privacidad.
- No tener un lugar seguro y de acceso restringido en donde se puedan archivar los datos personales en físico.
- Permitir a todo servidor público o personas ajenas a la dependencia, el acceso a los expedientes que contienen datos personales.
- Pérdida de expedientes físicos debido a catástrofes, inundaciones, e incendios.
- Daño de la base de datos que contenga información confidencial.
- Fallas en los equipos de cómputo en donde se encuentran las bases de datos.
- Falta de capacitación de los servidores públicos en relación con la confidencialidad que deben guardar sobre los datos personales que conozcan debido al desempeño de sus funciones.

- Pérdida, robo o extravío de expedientes.
- Alteración de la información.

Ante dichos riesgos identificados es necesario hacer un análisis de dichos riesgos, amenazas y sus posibles vulneraciones.

Origen de la amenaza	Causa	Posibles consecuencias
Acceso de personas no autorizadas a los sistemas o plataformas oficiales de la Honorable Junta Municipal de Constitución.	Adquirir información o datos personales.	Acceso no autorizado. Divulgación de datos personales. Modificaciones no autorizadas. Robo de información.
Acceso de personas no autorizadas como criminales o traficantes de datos a los sistemas o plataformas oficiales de la Honorable Junta Municipal de Constitución.	Adquirir datos personales para utilizarlos con fines de explotación, chantaje, extorsión o cualquier uso criminal.	Extorsiones. Ataques a personas. Robo de información. Vulneración a la seguridad física y mental de los ciudadanos.
Personal del sujeto obligado con poco conocimiento sobre el tratamiento de datos personales.	Obtener información para beneficio personal. Curiosidad. Error involuntario. Por fines económicos.	Ataque a otros servidores públicos. Robo de información. Pérdida de datos personales. Uso indebido de datos personales. Uso ilícito de datos personales. Extorsión. Modificaciones no autorizadas.
Daño físico.	Agua. Fuego. Accidentes. Corrosión.	Daño o pérdida de los datos personales.
Eventos naturales.	Desastres climatológicos. Fenómenos meteorológicos. Sismos. Cualquier eventualidad por causa natural.	Daño o pérdida de los datos personales.

Fallas técnicas.	Pérdida de electricidad. Falla o pérdida de internet. Falla en sistemas, correos electrónicos o plataformas oficiales.	Daño o pérdida de los datos personales. Divulgación y transferencia de datos personales. Modificaciones no autorizadas.
Desgaste Técnico.	Mantenimiento insuficiente. Falla en equipos. Poca o absoluta renovación de equipos de Telecomunicaciones o cómputos. Cambios de voltaje.	Pérdida, destrucción y daño.
Susceptibilidad en redes o sistemas autorizados.	Falta de contraseñas altamente efectivas. Falta de mecanismos para identificar o autenticación de usuarios. Falta de actualización de antivirus.	Pérdida, destrucción y daño. Divulgación y transferencia de datos personales. Modificaciones no autorizadas. Robo de información.
Organización.	Procesos carentes de formalidad para administración, acceso, uso y proceso de archivo.	Pérdida, destrucción y daño. Divulgación y transferencia de datos personales. Modificaciones no autorizadas. Robo de información.
Espacio donde se archiven.	Carencia de espacio. Espacio con poca seguridad. Espacio no adecuado. Falta de llaves o medidas de seguridad para accesos.	Daño o pérdida de los datos personales. Divulgación y transferencia de datos personales. Modificaciones no autorizadas. Robo de información.

Daño y/o alteración de la base de datos que contenga información confidencial.	Carencia de un servidor o sistema que almacene los datos personales. La falta de registros, controles o bitácoras, para regular la entrada y salida de personal autorizado, al área donde se almacenan o archivan los datos personales (en su caso los expedientes que los contengan), es un escenario de vulneración y riesgo, facilitando el mal manejo de los datos personales y la pérdida, robo o extravío de expedientes.	Daño y/o pérdida de los datos personales. Modificaciones no autorizadas.

Hasta el momento no se han identificado o reportado vulneraciones desde las áreas generadoras de información o las dependencias que integran la Honorable Junta Municipal de Constitución.

VIII. DEL ANÁLISIS DE BRECHA

Una vez identificados los posibles riesgos a los que este Sujeto Obligado se encuentra susceptible de enfrentar, podemos realizar el análisis de brecha, utilizando como base las entrevistas que se hicieron con cada enlace administrativo que tiene la Unidad de Transparencia de la Honorable Junta Municipal de Constitución.

Las áreas administrativas reportaron las siguientes medidas de seguridad existentes:

- Quien recaba los datos personales, es un servidor público del área, asignado especialmente para recabar datos en general necesarios para cada trámite.
- El espacio físico o área donde se recaban datos personales, es dentro de las instalaciones.
- Cuando los datos personales son recabados de forma digital, se realiza por medio de plataformas oficiales o correo electrónico oficial.
- En la mayoría de las áreas, el acceso (al área donde se recibe a los ciudadanos y se recaban datos personales) se tiene restringido, una vez que el dato se encuentra en posesión del servidor público.
- Una vez recabados los datos personales, el servidor público genera un expediente para cada trámite o servicio, del cual se obtuvieron los datos personales, ya sea físico o electrónico.

- Una vez recabados los datos personales, ya realizada la carpeta o expediente (electrónica, física, en plataformas, o cualquiera generada) y guardada esta en archiveros o puesta en resguardo electrónico, tienen acceso a esta área servidores públicos del área.
- Una vez recabados los datos personales, en caso de que se les dé proceso electrónico, el servidor público guarda los mismos en carpeta electrónica, ya sea en su computadora, carpeta compartida, correo electrónico oficial o plataforma.
- Durante el desahogo del trámite del cual se obtuvieron los datos personales, los servidores públicos del área tienen acceso a los datos personales.
- Una vez concluido el trámite, los datos personales recabados se dejan intactos en la carpeta, archivo o expediente del trámite al que pertenecen.
- Cada carpeta de trámites o archivo, al terminar el proceso de cada uno, son resguardados en un archivo de cada área.

Las medidas de seguridad que actualmente se llevan a cabo pudieran ser efectivas de aplicarse de manera continua y consciente en las áreas administrativas del sujeto obligado

El riesgo latente que se provoca por la falta de conocimiento, o compromiso para la aplicación de estas medidas existentes se puede minimizar por medio del establecimiento obligatorio de dichas medidas de seguridad y de la mejora continua de las mismas.

IX. DE LAS MEDIDAS DE SEGURIDAD

Con base en lo anterior se establecen las siguientes medidas de seguridad de carácter físico, técnico y administrativo:

Objetivo de control	Descripción
Control de servidores públicos que recaban los datos personales.	Debe realizarse un listado de los servidores públicos que recaban datos personales, esto es, de los servidores públicos que tienen contacto con el titular de los datos personales por sus funciones. (Quien recabe los datos generales para el trámite a realizar). Capacitaciones en materia de datos personales impartida por las áreas correspondientes de Transparencia. Remitir el documento de seguridad para el conocimiento y cumplimiento de las medidas de seguridad aplicables para un correcto tratamiento de datos personales.

Obtención de datos.	Para evitar el riesgo de obtener datos personales incompletos o incorrectos, el servidor público autorizado para recabarlos, deberá pedir al ciudadano acredite su personalidad.
Aviso de privacidad.	El servidor público que reciba los datos personales, deberá tener a la vista de todos los ciudadanos el aviso de privacidad, y darlo a conocer al momento de la recepción del trámite. Si el trámite del cual se recabarán datos personales, cuenta con un formato, este deberá contener la mención y debe dar a conocer el aviso de privacidad de la Honorable Junta Municipal de Constitución, ya sea simplificado, integral(físico) o la liga de internet que remita al ciudadano al aviso de privacidad simplificado o integral. Los formatos nuevos que se impriman posteriores a la emisión del presente documento deberán contar con la liga al aviso de privacidad o en su defecto el aviso de privacidad simplificado. Si el trámite del cual se recabarán datos personales, fue recabado mediante una plataforma electrónica oficial, esta plataforma deberá contener la mención y debe dar a conocer el aviso de privacidad, ya sea simplificado o la liga de internet que remita al ciudadano al aviso de privacidad integral.
Espacio físico.	Los datos personales recabados deberán ser recibidos únicamente en las instalaciones de cada área. El área específica donde se recaben los datos personales deberá contar con puertas que tengan llave, sin excepción alguna, para asegurar de forma efectiva el trato adecuado de los datos personales, así evitar mal uso de los mismos o vulneraciones. Al concluir la jornada laboral, se deberá guardar los expedientes, para no dejarlos al alcance de ciudadanos o personal no autorizado.
Resguardo provisional, durante el desahogo del trámite	Una vez recabados los datos personales, al generar el expediente (derivado del trámite), este deberá ponerse en algún lugar que esté fuera del alcance de los ciudadanos, ya sea en una caja, archivero, o mueble.

Archivo, al finalizar el desahogo del trámite	Al finalizar el desahogo de los expedientes estos deberán archivarse en un lugar adecuado con las siguientes características: • No estar al alcance de los ciudadanos • Deberá ser un área específica para guardar los expedientes.
Acceso al archivo.	Se deberá crear por cada área, un control o bitácora de los servidores públicos que tienen acceso al archivo.
Control de archivos electrónicos.	Cuando los datos personales sean recabados por medios electrónicos, se deberá generar expediente por cada trámite, dicho expediente deberá ser guardado en base de datos, correo electrónico oficial, o en plataforma autorizada, no en cualquier plataforma o correo electrónico personal. Para evitar riesgos, respecto a los expedientes electrónicos, se debe contar con un respaldo electrónico. Dicho respaldo deberá realizarse, como mínimo, de manera anual.
Inventarios Documentales sobre archivos.	Cada área del sujeto obligado deberá elaborar controles de archivo, conforme a sus procesos institucionales.
Transferencia de datos personales.	En caso de ser necesario derivado de las funciones de los servidores públicos, o por requisito del trámite, se deba realizar una transferencia de datos personales, se deberá informar al sujeto que reciba los datos el aviso de privacidad para que se sujete al mismo.
Versiones Públicas	En los casos en los cuales se realicen clasificaciones de información confidencial, que incluyan datos personales, los documentos que contengan los datos, deberán entregarse siempre en versión pública, adjuntando índice de datos personales.
Archivo finalizado	Al momento de finalizar el trámite, todos los expedientes, deberán desecharse y enviarse al archivo general, conforme a la normatividad correspondiente.

IX.1. Medidas de seguridad para transferencias:

a) Transferencias al interior del sujeto obligado y a otros sujetos obligados:

- Solo podrán ser transferidos los datos personales para dar seguimiento y conclusión al trámite o sistema de tratamiento bajo la finalidad que éstos prevean.
- El área que entrega los datos personales deberá cerciorarse de transferir la totalidad de los datos que resulten necesarios para el seguimiento o la conclusión del trámite o sistema de tratamiento correspondiente. Limitándose a la entrega de datos adicionales que no resulten necesarios.
- El área que entrega los datos personales deberá cerciorarse de que los datos que transfiere sean completos y veraces.
- El área que reciba los datos personales deberá conservar los mismos sujetándose a las finalidades y lineamientos del aviso de privacidad de este sujeto obligado y adoptando las medidas de seguridad previstas en este documento.
- El área que reciba los datos personales deberá encargarse de la supresión de los datos que reciba cuando esta corresponda.
- El área que entrega y el área que recibe los datos personales deberán dar acceso a los datos personales en tratándose de procedimientos de derecho ARCO.

b) Transferencias a terceros:

- El tercero que reciba los datos personales deberá sujetarse a las finalidades y lineamientos del aviso de privacidad de este sujeto obligado y deberá adoptar las medidas de seguridad previstas en este documento.
- En caso de ser necesario conforme a las disposiciones normativas, se deberá firmar un convenio o acuerdo de confidencialidad que proteja el tratamiento de los datos personales que recaba este sujeto obligado y transfiere al tercero.

IX.2. Medidas de seguridad en caso de vulneraciones a la seguridad:

En caso de ocurrir alguna vulneración deberá registrarse en la bitácora de contingencias, misma que deberá seguirse bajo el siguiente formato y ejemplo:

Fecha en la que ocurrió	***Motivo***	***Las acciones correctivas implementadas de forma inmediata y definitiva***
10/02/2022	*Huracán.*	*Impresión del expediente.* *Generar nuevo expediente electrónico.*

Después del registro, se deberá informar de forma inmediata al titular las vulneraciones de seguridad ocurridas, las que afecten o impacten de forma significativa los derechos patrimoniales o morales del titular, en un plazo máximo de setenta y dos horas en cuanto se confirmen y este en proceso las acciones encaminadas para dimensionar la afectación, con la finalidad de que los titulares

Puedan tomar medidas correspondientes para la defensa de sus derechos, dicha notificación debe contener lo siguiente:

1. La naturaleza del incidente.
2. Los datos personales comprometidos.
3. Las recomendaciones y medidas que el titular puede adoptar para proteger sus intereses.
4. Las acciones correctivas realizadas de forma inmediata.
5. Los medios donde puede obtener mayor información al respecto.

Al ocurrir una vulneración de seguridad, el servidor público titular del área responsable y/o el responsable del sistema deberá analizar la causa por lo que ocurrió dicha vulneración, e implementar y anexar a su plan de trabajo las acciones preventivas y correctivas para adecuar medidas de seguridad que prevengan esta eventualidad, para evitar que la vulneración se repita.

A su vez, en caso de detectar que la falla fue ocasionada por el incumplimiento de un servidor público a su cargo deberá levantar acta circunstanciada de hechos correspondiente y seguir el procedimiento administrativo correspondiente ante el Órgano Interno de Control de la Honorable Junta Municipal de Constitución.

IX.3. Medidas de seguridad o controles para la identificación y autentificación de usuarios

Parte de tener control efectivo al trato de los datos personales es contar con un sistema que garantice la autenticación de usuarios, esto es por medio de administración de cuentas creadas específicamente para cada servidor público.

La administración de cuentas de usuario es una parte esencial de los sistemas que se desarrollan en el departamento de software. La razón principal de las cuentas de usuario es verificar la identidad de cada funcionario también permite la utilización personalizada de acceso a la información y generación de la misma.

Esta medida es tomada para los correos electrónicos institucionales y para cualquier sistema o plataforma tecnológica que cree este sujeto obligado.

El estándar para la creación de las cuentas es:

Usuario: Generalmente es el correo electrónico institucional.
Contraseña: Frase de confirmación de identidad que se encuentra encriptado para mayor seguridad.

IX.4.- Medidas de seguridad para la supresión y borrado seguro de datos personales

Todos los datos personales en posesión del sujeto obligado sin importar el soporte en el que se encuentren deberán ser tratados para la supresión y borrado conforme a lo establecido en la Ley de Transparencia y Acceso a la Información Pública del Estado de Campeche, ya que el mismo tiene como uno de sus propósitos ser una guía para la operación de eliminación de archivos.

De conformidad con el artículo 32 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Campeche, el bloqueo se dará únicamente después del cumplimiento de la finalidad con la que fueron recabados los datos personales hasta que cumpla el plazo de prescripción legal o contractual correspondiente, concluido éste se deberá proceder a la supresión en la base de datos, archivo, registro, expediente que corresponda, al mismo tiempo se está garantizando la supresión de los datos personales.

Ahora bien especificaremos los objetivos de contar con técnicas apropiadas para la supresión y borrado de datos personales:

- Que la supresión y borrado de los expedientes que contengan datos personales sea de forma legal.
- Que la supresión y borrado de los expedientes que contengan datos personales sea de forma operativa conforme a los procedimientos utilizados en la Honorable Junta Municipal de Constitución.

Este apartado es el conjunto de estructuras para el proceso de supresión y borrado de los expedientes que contengan datos personales en posesión del sujeto obligado; por lo tanto los datos personales deberán estar contenidos en archivos apegados a un orden lógico y cronológico.

X. DEL PLAN DE CONTINGENCIA

Ante la pérdida total o parcial de datos personales en posesión de este sujeto obligado, se debe contar con un plan de contingencia.

Con la evaluación de riesgos y la elaboración de las medidas de seguridad aplicables para prevenir las posibles vulneraciones a las que estamos expuestos, nos encontramos con que el plan de contingencia de este sujeto obligado consiste en la aplicación de las medidas de seguridad tratadas en el apartado anterior, mismas que están sujetas a cambios por eventualidades no contempladas, por ello la importancia de señalar que el presente se trata de un plan de contingencia no limitativo.

Lo anterior toda vez que en la actualidad existen cambios y grandes avances que van modificando la organización de la información, y al igual existan riesgos inminentes que día a día evoluciona.

Con la aplicación de las medidas de seguridad establecidas en este documento se buscan minimizar los riesgos o vulneraciones, pero a su vez se intenta propiciar el restablecimiento de los datos personales en el menor tiempo posible ante cualquier eventualidad.

En caso de que los datos personales sufran algún tipo de daño o pérdida, se dispondrá de los respaldos electrónicos realizados por cada área administrativa en donde se contienen copias de documentos y/o archivos y/o bases de datos que contienen datos personales que permitirían restablecer los datos a la fecha del último respaldo.

XI. DEL PLAN DE TRABAJO

La existencia del documento de seguridad, busca enmarcar los deberes de la Honorable Junta Municipal de Constitución, para la máxima protección de datos personales. Debido a la importancia y el contexto actual en materia de datos personales, se debe mantener actualizado el plan de trabajo, el cual permita alcanzar los objetivos del sistema de seguridad de protección de datos personales.

La finalidad de este plan es plasmar de manera enunciativa, más no limitativa, las actividades que la Honorable Junta Municipal de constitución, realizará para la aplicación del presente documento de seguridad.

Lo anterior se realizará en base a las atribuciones establecidas en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Campeche.

Para la ejecución del presente documento de seguridad, dentro de los 6 meses siguientes a la emisión y aprobación del presente documento:

1. Se emitirá circular para difundir la emisión del presente documento, a través de la cual se remitirá copia digital del mismo a todos los correos institucionales vigentes.
2. Se comunicará a los enlaces sobre la emisión del documento de seguridad, solicitando su apoyo para la difusión interna del mismo.

El Comité de Transparencia revisará de manera anual, a partir de la emisión del presente documento de seguridad:

1. Revisar lo concerniente al índice de Datos Personales y mantenerlo actualizado.
2. Actualizar las medidas de Seguridad conforme al Sistema de Protección de Datos Personales hecho para la Honorable Junta Municipal de Constitución..
3. Integrarse al Plan de Trabajo que implemente la Unidad de Transparencia en materia de Protección de Datos Personales.

4. Integrarse al Programa Anual de Capacitaciones que genera la Unidad de Transparencia, además de promover que el personal de la Honorable Junta Municipal de constitución, se mantenga capacitado no sólo por sus áreas internas, sino también mediante su asistencia a capacitaciones otorgadas por organismos competentes en la materia.

XII. LOS MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

Se debe realizar un monitoreo y revisión de la aplicación de las medidas de seguridad, para valorar las amenazas, vulnerabilidades, aplicación correcta o incorrecta, impacto y actualización. Esto con el objetivo de que las medidas de seguridad continúan siendo efectivas e idóneas para el organismo.

Realizaremos el siguiente cuadro, donde se concentran los mecanismos de monitoreo y el objetivo de cada uno de ellos:

Mecanismos de monitoreo.	Objetivo del monitoreo.
Visitas a áreas elegidas de forma aleatoria.	Verificar de primera mano la aplicación, actualización e impacto de las medidas de seguridad aplicadas.
Pedir reportes a los responsables de cada área generadora de información o a los responsables del sistema de datos personales o a sus administradores sobre el manejo de datos personales conforme a las medidas de seguridad.	Monitorear y monitorear avances, aplicación, eventualidades y novedades respecto a la aplicación de las medidas de seguridad.

XIII. EL PROGRAMA GENERAL DE CAPACITACIÓN

Se manejarán las capacitaciones de conformidad al calendario que se emita por parte de la Unidad de Transparencia y en apego a las necesidades del sujeto obligado, es decir, la Honorable Junta Municipal de Constitución.