DOCUMENTO DE SEGURIDAD PARA LA PROTECCIÓN DE DATOS PERSONALES DE LA CONSEJERÍA JURÍDICA DEL PODER EJECUTIVO DEL ESTADO DE CAMPECHE.

CONTENIDO

INTRODUCCIÓN

El presente Documento de Seguridad se elabora de conformidad con lo establecido en el artículo 55 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Campeche, que establece como obligación que el sujeto responsable deberá elaborar y aprobar un documento que contenga medidas de seguridad de carácter físico, técnico y administrativo.

En la Consejería Jurídica del Poder Ejecutivo del Estado la información es un activo que debe protegerse mediante un conjunto de procesos y sistemas diseñados, administrados y mantenidos por la organización. De esta manera, la gestión de la seguridad de la información, como parte de un sistema administrativo más amplio, busca establecer, implementar, operar, monitorear y mejorar los procesos y sistemas relativos a la confidencialidad, integridad y disponibilidad de la información, aplicando un enfoque basado en los riesgos que la organización detecte.

El Documento de Seguridad es un instrumento que establece las medidas y procedimientos administrativos, físicos y técnicos de seguridad aplicables a los sistemas de datos personales necesarios para garantizar que éstos sean tratados conforme a los principios de licitud, consentimiento, calidad de los datos, confidencialidad, seguridad, disponibilidad y temporalidad. En este sentido, el Documento de Seguridad expone con detalle la estructura de organización, señala los puestos y la relación que existe entre ellos, la jerarquía, el grado de autoridad y responsabilidad, así como las funciones de los mismos, lo cual permitirá adoptar medidas idóneas para el tratamiento de los datos personales en posesión de la Consejería Jurídica del Poder Ejecutivo del Estado.

En ese tenor, este Documento de Seguridad tiene como finalidad proteger los datos del personal que labora en esta Consejería de posibles incidencias que puedan provocar su pérdida, alteración u acceso no autorizado, tanto interno como externo, por lo que permitirá, mediante su cumplimiento, garantizar niveles altos de seguridad en el tratamiento de dicha información.

Así, este documento pretende visibilizar, de forma clara y objetiva, a directivos y personal operativo de la Consejería Jurídica las medidas de seguridad que han sido tomadas para el resguardo de sus datos personales.

Este Documento de Seguridad que describe las medidas de seguridad, así como el personal autorizado y niveles jerárquicos de la Dependencia, variará en la medida que existan modificaciones al interior de esta Secretaría, por lo que es necesaria su revisión y actualización permanente para que cumpla cabalmente con su propósito.

GLOSARIO

I. **Áreas:** Instancias de los sujetos obligados previstas en los respectivos reglamentos interiores, estatus orgánicos o instrumentos equivalentes, que cuentan o pueden contar, dar tratamiento, y ser responsables o encargados de los datos personales;

II. **Base de datos:** conjunto ordenado de datos personales referentes a una persona física identificada o identificable, condicionado a criterios determinados que permitan su tratamiento, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización;

III. **Bloqueo:** la identificación y conservación de datos personales una vez cumplida la finalidad para la cual fueron recabados, con el único propósito de determinar posibles responsabilidades en relación con su tratamiento, hasta el plazo de prescripción legal o contractual de éstas. Durante dicho periodo, los datos personales no podrán ser objeto de tratamiento; transcurrido éste, se procederá a su supresión en la base de datos, archivo, registro, expediente o sistema de información que corresponda;

IV. **Comité de Transparencia:** instancia a que se refiere el artículo 48 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Campeche;

V. **Consentimiento:** manifestación de la voluntad libre, específica e informada de la persona titular, mediante la cual autoriza el tratamiento de sus datos personales;

VI. **Datos personales:** cualquier información concerniente a una persona física identificada o identificable expresada en forma numérica, alfabética, alfanumérica, gráfica, fotográfica, acústica o en cualquier otro formato. Se considera que una persona es identificable cuando su identidad puede determinarse, directa o indirectamente, a través de cualquier información, siempre y cuando esto no requiera plazos, medios o actividades desproporcionadas;

VII. **Datos personales sensibles:** aquellos que se refieren a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. Se consideran sensibles, de manera enunciativa más no limitativa, los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud pasado, presente o futuro, creencias religiosas, filosóficas y morales, opiniones políticas, datos genéticos, datos biométricos y preferencia sexual;

VIII. **Derechos ARCO:** los derechos de acceso, rectificación y cancelación de datos personales, así como la oposición al tratamiento de los mismos;

IX. **Disociación:** el procedimiento mediante el cual los datos personales no pueden asociarse a la o el titular ni permitir, por su estructura, contenido o grado de desagregación, la identificación del mismo;

X. **Documento de Seguridad:** instrumento que describe y da cuenta, de manera general, sobre las medidas de seguridad de carácter técnico, físico y administrativo adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee;

XI. **Encargado:** la persona física o jurídica colectiva, pública o privada, ajena a la organización del responsable, que sola o conjuntamente con otras trate datos personales a nombre y por cuenta del responsable;

I. **Evaluación de impacto a 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 previstas en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Campeche y demás normatividad aplicable en la materia;

II. **Fuentes de acceso público:** aquellas bases de datos, sistemas o archivos que, por disposición de la Ley local en la materia y demás normatividad aplicable, puedan ser consultadas públicamente cuando no exista impedimento por una norma limitativa y sin más exigencia que, en su caso, el pago de una contraprestación, tarifa o contribución. No se considerará fuente de acceso público cuando los datos personales contenidos en la misma sean obtenidos o tengan una procedencia ilícita, conforme a las disposiciones establecidas en la legislación y normatividad aplicable en la materia;

III. **Ley:** Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Campeche;

IV. **Ley de Transparencia:** Ley de Transparencia y Acceso a la Información Pública del Estado de Campeche;

V. **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;

VI. **Medidas de seguridad administrativas:** políticas y procedimientos para la gestión, soporte y revisión de la seguridad de los datos personales a nivel organizacional, la identificación, clasificación y borrado seguro de los datos personales, así como la sensibilización y capacitación del personal en materia de protección de datos personales;

VII. **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. De manera enunciativa más no limitativa, se deberán considerar las siguientes actividades:

   a. Prevenir el acceso no autorizado al perímetro de la organización del responsable, sus instalaciones físicas, áreas críticas, recursos y datos personales;
   b. Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la organización del responsable, recursos y datos personales;
   c. Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pudiera salir de la organización del responsable, y

d. Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz, que asegure su disponibilidad e integridad;

VIII. **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 los recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se deberán considerar las siguientes actividades:

a. Prevenir que el acceso a los datos personales, así como a los recursos, sea por usuarios identificados y autorizados;
b. Generar un esquema de privilegios para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones;
c. Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware, y
d. Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales;

IX. **Remisión:** toda comunicación de datos personales realizada exclusivamente entre el responsable y el encargado, con independencia de que se realice dentro o fuera del territorio mexicano;

X. **Responsable:** cualquier autoridad, dependencia, entidad, órgano y organismo de los poderes Legislativo, Ejecutivo y Judicial, ayuntamientos, órganos, organismos constitucionales autónomos, tribunales administrativos, fideicomisos y fondos públicos y partidos políticos del orden estatal y municipal del Estado de Campeche, que decide y determina los fines, medios y demás cuestiones relacionadas con determinado tratamiento de datos personales;

XI. **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;

XII. **Titular:** persona física a quien corresponden los datos personales;

XIII. **Transferencia:** toda comunicación de datos personales dentro o fuera del territorio mexicano, realizada a persona distinta del titular, del responsable o del encargado;

XIV. **Tratamiento:** cualquier operación o conjunto de operaciones efectuadas mediante procedimientos físicos o automatizados aplicados a los datos personales, relacionados, de manera enunciativa más no limitativa, con la obtención, uso, registro, organización, conservación, elaboración, utilización, estructuración, adaptación, modificación, extracción, consulta, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, transferencia y, en general, cualquier uso o disposición de datos personales;

XV. **Transmisión de datos personales**. La entrega total o parcial de sistemas de datos personales a cualquier persona distinta de la o el titular de los datos, mediante el uso de medios físicos o electrónicos, tales como la interconexión de computadoras o

bases de datos, acceso a redes de telecomunicación, así como a través de la utilización de cualquier otra tecnología que lo permita.

XVI. **Usuario**: servidora o servidor público facultado por un instrumento jurídico, o expresamente autorizado por el Responsable, que utiliza de manera cotidiana datos personales para el ejercicio de sus atribuciones.

MARCO JURÍDICO

- Constitución Política de los Estados Unidos Mexicanos.
- Constitución Política del Estado de Campeche.
- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
- Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Campeche.
- Lineamientos para la Protección de Datos Personales en Posesión de Sujetos Obligados en el Estado de Campeche.
- Guía para la elaboración de un Documento de Seguridad v1.4 del Instituto Nacional de Transparencia y Acceso a la Información y Protección de Datos Personales.

AMBITO DE APLICACIÓN

El presente Documento de Seguridad es aplicable y de observancia obligatoria para todas las unidades administrativas de la Consejería Jurídica del Poder Ejecutivo del Estado de Campeche, en cumplimiento de sus funciones inherentes conforme a su reglamento interior, así como para las personas externas que, debido a la presentación de un servicio, tengan acceso a tales sistemas o al sitio donde se ubican los mismos.

MEDIDAS DE SEGURIDAD IMPLEMENTADAS

Es importante aclarar las diferencias existentes entre las medidas de seguridad administrativas, físicas y técnicas, con el fin de enunciar los elementos teóricos utilizados en la elaboración del presente Documento de Seguridad.

a) Las medidas de seguridad administrativas 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 físicas 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 técnicas son las aplicables a sistemas de datos personales en soportes electrónicos, servicios e infraestructura de telecomunicaciones y tecnologías de la información, entre otras, y 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 como para la gestión interna como para la que se lleva a cabo con terceros. Incluye, entre otros aspectos, la 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, la 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 el procesamiento adecuado en las aplicaciones, controles criptográficos y seguridad de los archivos de sistema, entre otros.

• Tipo de soportes: físicos y electrónicos. Es importante explicar la diferencia entre un soporte físico y un soporte electrónico, debido a que las medidas de seguridad que este sujeto obligado implementa para cada sistema de datos personales está estrechamente relacionado 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 medios de almacenamiento inteligibles que sólo mediante el uso de algún aparato con circuitos electrónicos se puede procesar 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.

PROCEDIMIENTO DE RESPALDO Y RECUPERACIÓN DE DATOS PERSONALES

Se considera como el procedimiento implementado para el resguardo de datos o documentos, realizado con la finalidad de prevenir su perdida en caso de imprevistos en los sistemas informáticos. Por ejemplo, el caso de los discos duros, ya que son instrumentos delicados y con una probabilidad más alta de presentar fallos.

Un respaldo de información bien organizado y estructurado permite la posibilidad de acceder nuevamente a los documentos contenidos y necesarios de resguardar, evitando de ese modo que la información importante se pierda.

Los procedimientos de respaldo y recuperación desarrollados deben formar parte de un plan de respaldo y recuperación, el cual debe ser documentado y en el que es pertinente señalar lo siguiente:

- Señalar si es un respaldo completo, diferencial o incremental;
- El tipo de medios utilizados para su almacenaje;
- El modo y el lugar en que se han de archivar los medios; y
- Señalar a la o el Responsable de la realización de esas operaciones (el sujeto obligado o un tercero).

Asimismo, y ya que a lo largo del tiempo varias características que se consideran para desarrollar este plan sufren cambios (software utilizado, soporte, etc.), el plan debe ser revisado y, en caso de ser necesario, modificado de manera periódica.

INVENTARIO Y CATÁLOGO DE DATOS PERSONALES

A continuación, se describen las categorías de datos personales con los que cuenta la Consejería Jurídica del Poder Ejecutivo del Estado de Campeche, de acuerdo con las facultades que tiene señaladas en la Ley Orgánica de la Administración Pública Estatal y su Reglamento Interior.

Datos de Identificación y contacto: Nombre, estado civil, RFC, CURP, copia de credencial de elector, lugar de nacimiento, fecha de nacimiento, nacionalidad, domicilio particular, teléfono particular, teléfono celular, correo electrónico, firma autógrafa, edad, fotografía y referencias personales.

Datos laborales: Puesto o cargo que desempeña, nombramiento, constancia de no inhabilitación para el empleo, actividades extracurriculares, *curriculum vitae*, domicilio de

trabajo, correo electrónico institucional, teléfono institucional, referencias laborales, información generada durante los procesos de selección y contratación y experiencia/capacitación laboral.

Datos Patrimoniales: Bienes muebles e inmuebles, información fiscal, ingresos y egresos, cuentas bancarias y seguros contratados.

Datos Académicos: Último grado de estudios, trayectoria académica, evaluaciones, títulos, cédula profesional, certificados o constancias escolares.

Datos de Salud: Certificado médico, incapacidades médicas, referencias o descripción de sintomatologías, intervenciones quirúrgicas, detección de enfermedades y consumo de medicamentos.

Datos Biométricos: Huellas dactilares**.**

Datos Afectivos y/o Familiares: Estado civil, número de hijos, nombres de familiares dependientes económicos, beneficiarios, referencias familiares, parentesco.

Datos Personales de Naturaleza Pública: Aquellos que por mandato legal expreso sean accesibles al público, por ejemplo; nombre y percepciones de servidores públicos.

PROCEDIMIENTO DE OBTENCIÓN DE LOS DATOS PERSONALES

Este sujeto obligado obtiene los datos personales señalados con anterioridad de las y los servidores públicos que laboran en esta Consejería Jurídica, personas físicas y/o morales que se contratan para la prestación de un servicio profesional, así como estudiantes que realizan su servicio social por un periodo determinado.

Los datos personales se recaban por medio de documentos presentados y/o por el llenado de formularios físicos realizados por las y los titulares de los datos personales.

La recepción de esos documentos se realiza en la Coordinación de Administración de la Consejería Jurídica, la cual se encarga de su resguardo y posterior llenado de los formatos autorizados por la Dirección de Administración de Personal de la Secretaría de Administración e Innovación Gubernamental para trámites de nuevo ingreso. Los formatos se entregan en original junto con los documentos personales en original y/o copia a la Dirección de Administración de Personal de la Secretaría de Administración e Innovación Gubernamental. La Consejería Jurídica del Poder Ejecutivo del Estado de Campeche deja bajo su resguardo copia fotostática de la documentación remitida a la Dirección señalada con anterioridad.

TIPO DE TRANSMISIONES DE DATOS PERSONALES Y MODALIDADES PARA LA TRANSMISIÓN

Una transmisión de datos personales implica la entrega total o parcial de sistemas de datos personales a cualquier persona distinta de la o el titular de los datos, mediante el uso de medios físicos o electrónicos, tales como la interconexión de computadoras o bases de

datos, acceso a redes de telecomunicación, así como a través de la utilización de cualquier otra tecnología que lo permita.

En el caso de la Consejería Jurídica, únicamente realiza el siguiente tipo de transmisión:

> Interinstitucional: la cual consiste en la transmisión de datos a Dependencias y Entidades de la Administración Pública del Estado.

Para implementar las medidas de seguridad aplicables a la transmisión enunciada, la unidad administrativa responsable debe considerar la modalidad por la cual se envían los datos personales a los destinatarios, pudiendo hacerse el traslado mediante las siguientes modalidades:

a) **Traslado de soporte físicos:** En esta modalidad los datos personales se trasladan en medios de almacenamiento inteligibles a simple vista que no requieren de ningún aparato que procese su contenido para examinar, modificar o almacenar los datos. Un ejemplo de este traslado de soportes físicos es cuando una Dependencia envía por correspondencia oficios o formularios impresos.

b) **Traslado físico de soportes electrónicos:** En esta modalidad se trasladan físicamente, para entregar al destinatario, los datos personales en archivos electrónicos contenidos en medios de almacenamiento inteligibles que sólo mediante el uso de algún aparato con circuitos electrónicos que procese su contenido se puede examinar, modificar o almacenar los datos. Un ejemplo de ello es cuando una Dependencia entrega a otra, por mensajería oficial, un archivo electrónico con datos personales contenidos en discos flexibles, discos compactos o dispositivos de memoria USB, entre otros.

c) **Traslado sobre redes electrónicas:** En esta modalidad se transmiten los datos personales en archivos electrónicos mediante una red electrónica.

CATÁLOGO DE SISTEMAS DE DATOS PERSONALES

Unidad Administrativa:	**Coordinación de Administración**
Nombre del sistema:	**Administración de Recursos Humanos de la Consejería Jurídica del Poder Ejecutivo del Estado de Campeche**
Responsable	
Nombre:	**M.A. Manuel Jesús Méndez Córdova**
Cargo:	**Coordinador de Administración**
Funciones:	▪ Las señaladas en el artículo 19 del Reglamento Interior de la Consejería Jurídica. ▪ Las que se establecen en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Campeche. ▪ Las Establecidas en los lineamientos para la Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Campeche.
Obligaciones:	• Establecer controles o mecanismos para asegurar la confidencialidad de los datos personales. • Mantener y documentar las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales. • Establecer medidas de seguridad técnica y organizativa para garantizar la confidencialidad e integralidad de cada sistema de datos personales. • Crear políticas internas para la gestión y tratamiento de los datos personales. • Elaborar un inventario de datos personales. • Elaborar y aprobar un documento que contenga las medidas de seguridad de carácter físico, técnico y administrativo.
Encargado	
Nombre:	**C.P. Ángel Francisco Gómez González**
Cargo:	**Subdirector de Coordinación de Administración**
Funciones:	• Mantener la integridad, disponibilidad y confidencialidad de la información; así como dar cumplimiento a las medidas de seguridad previstas en el presente Documento de Seguridad para los Sistemas de Datos Personales en Medios Físicos. • Recabar cada uno de los documentos que se les solicita a las y los servidores públicos que laboran en la Consejería Jurídica.

Obligaciones:	• Supervisar el correcto resguardo de datos personales, de conformidad con lo establecido en el presente Documento de Seguridad y la normatividad en la materia. • Hacer uso de los datos únicamente para los fines para los cuales han sido recabados. • Garantizar la seguridad en el tratamiento de datos personales, con la finalidad de evitar algún riesgo, como la pérdida, robo, alteración o acceso no autorizado. • Garantizar el cumplimiento de los derechos ARCO a las y los titulares de los datos personales.
Usuaria	
Nombre:	**C.P. Zenaida del Carmen Arroyo Zubieta**
Cargo:	**Directora A**
Funciones:	• Apoyar en el archivo de la documentación que se genera diariamente, de acuerdo a las indicaciones del responsable del archivo. • Vigilar que, durante el desempeño de sus funciones, en el espacio físico destinado para el resguardo de los datos personales, no tengan acceso a esos datos personas no autorizadas. • Reportar a su autoridad inmediata superior sobre cualquier incidente que se presente en el resguardo, consulta, acceso o transmisión de los datos personales y, simultáneamente, hacer el registro correspondiente.
Obligaciones:	• Recabar cada uno de los documentos que se les solicita a las y los servidores públicos que laboran en la Consejería Jurídica. • Integrar y mantener resguardados los expedientes correspondientes. • Controlar el acceso, consulta y, en su caso, la transmisión de datos personales en el sistema de administración de recursos humanos. • Realizar el llenado correcto de la bitácora de registro diario sobre las consultas que se realicen por el personal autorizado. • Controlar que, durante el desempeño de sus funciones, en el espacio físico destinado para el resguardo de los datos personales, no tengan acceso a esos datos personas no autorizadas. • Reportar, de manera inmediata, a la o el responsable del sistema, sobre cualquier incidente que se

	presente en el resguardo, consulta, acceso o transmisión de los datos personales y, simultáneamente, hacer el registro correspondiente.
Folio de inscripción:	00108.00111.0175.20140129

ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE DATOS PERSONALES

Unidad Administrativa:	**Coordinación de Administración**
Nombre del Sistema:	**Administración de Recursos Humanos de la Consejería Jurídica del Poder Ejecutivo del Estado de Campeche**
TIPO DE SOPORTE	
Tipo de Soporte:	**Soporte Físico**
Descripción:	**Expedientes de Personal**
Características del lugar donde se resguardan los soportes	
Oficina con ventilación y luz artificial, puerta de acceso de madera y chapa, aislada de humedad, con archiveros y anaqueles que permiten la conservación adecuada de los documentos que contienen datos personales. Para el resguardo de los datos personales se utiliza un archivero metálico con caja fuerte, gavetas tamaño oficio con llave, con número de inventario 11802511104000086.	

MECANISMOS DE IDENTIFICACIÓN Y AUTENTIFICACIÓN

Sistemas Manuales

a) Elaboración de una relación actualizada de servidoras y servidores públicos y empleadas y empleados externos de la Consejería Jurídica del Poder Ejecutivo del Estado de Campeche.

b) Para el acceso se solicitará identificación con validez oficial, la cual será autentificada con el cotejo del listado de personal autorizado que se encuentra anexo a este Documento de Seguridad y/o lista de control de acceso (bitácora).

Sistemas Automatizados

a) Para el acceso se solicitará identificación con validez oficial, la cual será autentificada con el cotejo del listado de personal autorizado que se encuentra anexo a este Documento de Seguridad y/o bitácora.

Sólo tendrán acceso a este sistema la o el Responsable, la o el Encargado y la o el Usuario.

MECANISMOS DE CONTROL DE ACCESO

Sistemas Manuales

a) Elaboración de una relación actualizada de servidoras y servidores públicos y empleadas y empleados externos de la Consejería Jurídica del Poder Ejecutivo del Estado de Campeche; así como de las y los operarios autorizados.

b) Elaboración de Lista de control de acceso (bitácora).

c) Para el acceso se solicitará identificación con validez oficial, la cual será autentificada con el cotejo del listado de personal autorizado que se encuentra anexo a este Documento de Seguridad y/o lista de control de acceso (bitácora).

d) Será obligatorio, para el acceso a las áreas que cuenten con un Sistema Físico o Automatizado, el llenado de la lista de control de acceso antes y después del ingreso, aportando información clara y precisa de los expedientes utilizados.

Sistemas Automatizados

a) Elaboración de una lista actualizada de responsable y operarios autorizados de la Consejería Jurídica del Poder Ejecutivo del Estado de Campeche.

b) Elaboración de una Lista de control de acceso (bitácora).

c) Para el acceso se solicitará identificación con validez oficial, la cual será autentificada con el cotejo del listado de responsable y operarios autorizados que se encuentra anexo a este Documento de Seguridad y/o lista de control de acceso (bitácora).

d) Será obligatorio, para el acceso a las áreas que cuenten con un Sistema Físico o Automatizado, el llenado de la lista de control de acceso antes y después del ingreso, aportando información clara y precisa del sistema y soportes manejados.

Sólo tendrán acceso a este sistema la o el Responsable, la o el Encargado y la o el Usuario.
Sólo el Responsable del Sistema de Datos Personales podrá conceder, alterar o anular la autorización para el acceso a dichos sistemas.

MECANISMOS DE CONTROL DE ACCESO FÍSICO

Sistemas Manuales

a) Colocación de avisos visibles de acceso a personal sólo autorizado.

b) Colocación de aviso de Acceso Restringido en la instalación que contiene los Sistemas Físicos.

c) Colocación del aviso de privacidad.

d) Elaboración de una relación actualizada de servidores públicos y empleados autorizados.

b) Elaboración de Lista de control de acceso (Bitácora)

c) Para el acceso se solicitará identificación con validez oficial, la cual será autentificada con el cotejo del listado de personal autorizado.

Será obligatorio, para el acceso a las áreas que cuenten con un Sistema Físico o Automatizado, el llenado de la lista de control de acceso antes y después del ingreso, aportando información clara y precisa de los expedientes utilizados.

Acceso de terceras personas.

a) Colocación del aviso de privacidad para terceras personas en la entrada de la Dependencia y de la unidad administrativa.

b) Registro obligatorio de entrada y salida en la bitácora de visitas de la Consejería Jurídica, colocada a la entrada de la misma llenando todos los rubros.

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

Bitácoras de Acceso	1. Las bitácoras de acceso a los datos personales se utilizarán en los soportes físicos y contendrán la siguiente información: • Nombre y cargo de quien accede; • Identificación del Expediente; • Fojas del Expediente; • Propósito del Acceso; • Fecha de Acceso; • Hora de Acceso; • Fecha de Devolución; y • Hora de Devolución. 2. Las bitácoras se encontrarán en soporte físico. 3. Serán resguardadas por el responsable del área en el lugar que para tal efecto se designe, el cual debe estar resguardado bajo llave.

Vulneraciones a la Seguridad de los Datos Personales	**La bitácora de vulneraciones deberá contener la siguiente información** 1. Nombre de quien reporta el incidente; 2. Cargo; 3. La fecha en la que ocurrió; 4. El motivo de la vulneración de seguridad; y 5. Las acciones correctivas implementadas de forma inmediata y definitiva.

CONTROLES DE IDENTIFICACIÓN Y AUTENTIFICACIÓN DE USUARIOS

Las y los empleados de la Consejería Jurídica del Poder Ejecutivo del Estado de Campeche deben portar en todo momento su identificación institucional, misma que contará con la información siguiente:

Al frente:

- Nombre; y
- Cargo.

Al reverso:

- Vigencia;
- Número de Empleada o Empleado;
- Firma de la o el Titular de la Dependencia; y
- Sitio Oficial.

En el ambiente electrónico todas las computadoras precisan de un nombre de usuario y contraseña para ingresar.

TÉCNICAS DE SUPRESIÓN Y BORRADO SEGURO DE DATOS PERSONALES

Los medios considerados en el presente caso, por su eficacia al evitar completamente la recuperación de los datos contenidos en los dispositivos de almacenamiento, son la desmagnetización, la destrucción y la sobre-escritura en la totalidad del área de almacenamiento de la información.

Desmagnetización

La desmagnetización consiste en la exposición de los soportes de almacenamiento a un potente campo magnético, proceso que elimina los datos almacenados en el dispositivo.

Este método es válido para la destrucción de datos de los dispositivos magnéticos, por ejemplo, los discos duros, disquetes, cintas magnéticas de *backup*, etc. Cada dispositivo, según su tamaño, forma y el tipo de soporte magnético de que se trate, necesita de una potencia específica para asegurar la completa polarización de todas las partículas.

Destrucción física

El objetivo de la destrucción física es la inutilización del soporte que almacena la información en el dispositivo, con la finalidad de evitar la recuperación posterior de los datos que almacena. Existen diferentes tipos de técnicas y procedimientos para la destrucción de medios de almacenamiento, como son: la desintegración, pulverización, fusión e incineración, siendo métodos diseñados para destruir por completo los medios de almacenamiento. Estos métodos suelen llevarse a cabo en una destructora de metal o en una planta de incineración autorizada, con las capacidades específicas para realizar estas actividades de manera eficaz, segura y sin peligro.

Trituración: las trituradoras de papel se pueden utilizar para destruir los medios de almacenamiento flexibles. El tamaño del fragmento de la basura debe ser lo suficientemente pequeño para que haya una seguridad, razonable en proporción a la confidencialidad de los datos, de que no pueden ser reconstruidos.

Los medios ópticos de almacenamiento (CD, DVD, magneto-ópticos) deben ser destruidos por pulverización, trituración de corte transversal o incineración. Cuando el material se desintegre o desmenuce, todos los residuos se reducen a cuadrados de cinco milímetros (5mm) de lado. Como todo proceso de destrucción física, su correcta realización implica la imposibilidad de recuperación posterior por ningún medio conocido.

En el caso de los discos duros se deberá asegurar que los platos internos del disco han sido destruidos eficazmente, no sólo la cubierta externa.

Sobre-escritura

La sobre-escritura consiste en la escritura de un patrón de datos sobre los datos contenidos en los dispositivos de almacenamiento. Para asegurar la completa destrucción de los datos se debe escribir la totalidad de la superficie de almacenamiento. La sobre-escritura se realiza accediendo al contenido de los dispositivos y modificando los valores almacenados,

por lo que no se puede utilizar en aquellos que están dañados ni en los que no son regrabables, como los CD y DVD.

REGISTRO DE INCIDENCIAS

Las incidencias con datos personales que se puedan producir vulnerarían la debida protección de los mismos, por lo tanto, es necesario que la Coordinación de Administración de la Consejería Jurídica, en donde se da tratamiento a datos personales, lleve a cabo un registro de las incidencias que comprometen la seguridad de los datos.

El registro de incidencias deberá contener, por lo menos, lo siguiente:

I. La fecha de la incidencia, su el tipo y descripción:
II. La persona quien la registra; y
III. La persona a quien se la comunican las consecuencias que tendrá esa incidencia.

El personal de la Consejería Jurídica que trate datos personales deberá de contar con el registro de incidencias, ya que quien identifique la incidencia será el encargado de registrarla y notificar a su superior inmediato, quien, a su vez, se encargará de notificar a la o las personas afectadas para que se tomen las precauciones debidas en caso de uso inadecuado de la información.

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

El Sistema de Gestión de Seguridad de la Información (SGSI) es un sistema que identifica los diversos activos (personas, hardware, software, documentos, etc.) para llevar a cabo un análisis de los riesgos a los que pueden estar expuestos y, de ese modo, realizar acciones que permitan minimizar el impacto en caso de presentarse. Todo eso para garantizar la confidencialidad, la integridad y la disponibilidad de dichos activos.

En el Sistema de Gestión se deben documentar políticas, procesos, procedimientos, protocolos, formatos y demás actividades a fin de poder ser auditadas y, en su caso, llevar acciones correctivas, con la finalidad de tener un proceso de mejora continua. Por lo tanto, debe apegarse a lo siguiente:

- Gestionar las amenazas de la institución que puedan afectar el cumplimiento de los objetivos: esto implica la identificación, el análisis y el tratamiento de los riesgos.
- Contar con criterios y políticas específicas que permitan minimizar las amenazas que pudieran presentarse e impactar a los objetivos, institucionales, tácticos y operativos.
- Garantizar que la información mantenga su confidencialidad, su integridad y su disponibilidad, para su adecuada utilización.

ANÁLISIS DE RIESGOS

El proceso de análisis de riesgos considera la evaluación cuantitativa y cualitativa sobre la posibilidad de que un activo de información pueda sufrir una pérdida o daño. Contempla la identificación de activos, el estudio de causas y consecuencias de las amenazas y vulnerabilidades en los sistemas de tratamiento de datos personales, y permite establecer parámetros para ponderar los efectos de posibles vulneraciones de seguridad. Esta metodología en particular contempla tres factores que, en conjunto, determinan el riesgo latente de los datos personales. Tales factores son:

• **Beneficio:** factor que deriva en el nivel de riesgo por tipo de dato, determinado por el riesgo inherente del dato y el volumen de titulares de los que se tratan datos.

• **Accesibilidad:** factor que determina el nivel de riesgo por tipo de acceso, es decir, el número de accesos potenciales a los datos.

• **Anonimidad:** factor que determina el nivel de riesgo por tipo de entorno desde el que se tiene acceso a los datos.

Estos factores de riesgo nos permiten obtener un valor cuantitativo del nivel de riesgo latente de cada particular con relación al tratamiento de datos personales y sensibles y, a partir de ello, permite generar una lista de controles congruentes para disminuir los posibles impactos a los datos personales o sensibles.

ANÁLISIS DE BRECHA

La realización de un análisis de brecha va enfocado a la seguridad de los datos personales recabados, realizando un diagnóstico de las prácticas de seguridad de la información con las que cuenta, en ese momento, el sujeto obligado y las que deberían de tenerse con base a las mejores prácticas.

Las mejores prácticas deben de cubrir las áreas o dominios de la seguridad de la información, con la finalidad de que permitan evaluar e identificar, de manera amplia, las prácticas que se deberán de llevar a cabo para un mejor cumplimiento de las obligaciones en materia de protección de datos personales; de esta manera, se puede establecer el nivel de madurez de las prácticas realizadas por el sujeto obligado y, posteriormente, definir las acciones que se llevarán a cabo para disminuir la brecha entre la situación actual y las mejores prácticas.

Algunos de los aspectos a evaluar y ponderar para tener una visión más completa y concreta sobre el estado actual de la seguridad de los datos personales y los aspectos existentes son:

- **Seguridad institucional.**
  Control de la información compartida con terceros.
- **Activos del responsable**
  Asignación de responsabilidades y clasificación.
- **Seguridad en recursos humanos**

Cuidar la seguridad de los recursos humanos previo a la contratación, durante y una vez que haya culminado su trabajo.

- **Seguridad física y ambiental**
  Áreas seguras y protección de equipamiento.
- **Operación, procedimientos y comunicación**
- **Cumplimiento con leyes y lineamientos**
- **Control de acceso a la información**
  Derechos y control de acceso a aplicaciones, redes y sistemas operativos.

  Protección móvil y trabajo remoto.
- **Seguridad de sistemas de información**
  Procesos de información.

  Controles criptográficos.

  Protección de archivos de sistema.
- **Incidentes de seguridad de información**

De ese modo, se concluye que, actualmente, se tiene un nivel de medidas de seguridad óptimas en relación con los datos personales que se manejan.

Asimismo, con las medidas de seguridad señaladas en este Documento de seguridad, se pretende que éstas queden asentadas y uniformes.

MECANISMO DE MONITOREO Y REVISIÓN DE MEDIDAS DE SEGURIDAD

Todos los proyectos de la Consejería Jurídica del Poder Ejecutivo del Estado de Campeche de Protección de Datos Personales se componen de, como mínimo, las siguientes actuaciones:

- Análisis y diagnosis del tratamiento de la información y de los procedimientos de seguridad, así como de los de carácter organizativo, para verificar el cumplimiento de la normatividad.
- Elaboración de las propuestas de inscripción, modificación y/o supresión de ficheros de titularidad pública y privada de la Dependencia, así como los nombramientos de responsables de ficheros y de seguridad.
- Revisión y, en caso necesario, generación de los Documentos de Seguridad.
- Revisión y, en su caso, generación de las cláusulas legales y carteles informativos para cumplir con el deber de informar, obtener el consentimiento al tratamiento y la cesión de datos en los casos necesarios, y contratos con terceros.

PLAN DE TRABAJO

PROGRAMA DE CAPACITACIÓN EN DATOS PERSONALES

Alcance:

El presente plan de capacitación es aplicable para la mayoría de las y los servidores públicos que laboran en este sujeto obligado.

Fines del Plan de Capacitación:

Su propósito general es cumplir con la norma y mejorar los procesos de acceso a la información pública, así como la protección de los datos personales. Se pueden señalar como fines específicos los siguientes:

- Elevar el nivel de conocimiento de las y los servidores públicos en la materia.
- Satisfacer requerimientos futuros con base a la planeación del manejo de información y de datos personales.
- Generar conductas positivas y mejoras en la calidad del tratamiento de información y protección de datos personales.
- Cumplir con las disposiciones legales en la materia.
- Dar confianza a las personas acerca de la protección de su información y datos personales.

Objetivo General:

- Lograr el avance de la Consejería Jurídica del Poder Ejecutivo del Estado de Campeche en relación a la definición de sus políticas y mecanismos de aseguramiento de la calidad, consolidando una cultura de la evaluación y control, incorporando buenas prácticas en la gestión institucional, a partir de la instauración de procesos de evaluación permanente, planificación, seguimiento de resultados y ajuste constante de las actividades.
- Contribuir en la actualización, formación y profesionalización, de manera directa, de todas y todos los servidores públicos del sujeto obligado en el desempeño de esta actividad, en especial a las y los encargados de implementar las acciones para cumplir con la norma de protección de datos personales.

DE LOS PROGRAMAS DE CAPACITACIÓN Y ACTUALIZACIÓN

El personal de la Coordinación de Administración de la Consejería Jurídica conjuntamente con la Coordinación de Planeación, Capacitación y Apoyo Técnico, así como con el Comité de Transparencia, capacitarán a las y los servidores públicos de este sujeto obligado en materia de protección de datos personales, al menos, una vez al año.

En caso de que en el transcurso del año se presente alguna modificación a la ley de la materia, surja alguna actualización en el tema o alguna de las Unidades Administrativas tenga la necesidad de capacitación, se solicitará la programación del curso.

Asimismo, el personal de la Coordinación estará en capacitación constante, a través de cursos y/o talleres presenciales o en línea por parte de la Comisión de Transparencia y Acceso a la Información Pública del Estado de Campeche.

ACTUALIZACIÓN DEL DOCUMENTO DE SEGURIDAD

El presente Documento de Seguridad se actualizará cuando ocurran los siguientes eventos:

- Se produzcan modificaciones sustanciales al tratamiento de datos personales que deriven en un cambio en el nivel de riesgo;
- Como resultado de un proceso de mejora continua, derivado del monitoreo y revisión del sistema de gestión;
- Como resultado de un proceso de mejora para mitigar el impacto de una vulneración a la seguridad;
- Implementación de acciones correctivas y preventivas ante una vulneración a la seguridad;
- Cuando surjan documentos, formatos, recomendaciones, etc. por parte de la Comisión de Transparencia y Acceso a la Información Pública del Estado de Campeche, para la mejora del Documento de Seguridad.

APROBACIÓN DE DOCUMENTO DE SEGURIDAD

El Comité de Transparencia de esta Consejería Jurídica, en la décimo primera sesión extraordinaria, de fecha 26 de marzo de 2021, aprobó por unanimidad el presente Documento de Seguridad.