DOCUMENTO DE SEGURIDAD PARA LA PROTECCIÓN DE DATOS PERSONALES DE LA CONSEJERÍA JURÍDICA DEL PODER EJECUTIVO DEL ESTADO DE QUINTANA ROO

INDICE

I. INTRODUCCIÓN

La Consejería Jurídica del Poder Ejecutivo del Estado de Quintana Roo, en su calidad de responsable, a fin de dar cumplimiento al deber de seguridad y en completo apego a las disposiciones contenidas en el Capítulo II "De los Deberes" de la Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados del Estado de Quintana Roo, ha establecido un conjunto de procesos y sistemas diseñados para la protección de los datos personales a los cuales tenga acceso a su tratamiento de acuerdo a sus funciones y atribuciones de ley.

Para este Sujeto Obligado, 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.

En tal sentido, dentro de las acciones a emprender en toda institución para cumplir con dicho deber, se crea el documento de seguridad, instrumento que dará cuenta de todas las medidas, acciones, actividades, controles o mecanismos, implementados por el responsable con el objeto de garantizar que el tratamiento de los datos personales que realiza sea conforme a las disposiciones contenidas en la normatividad de la materia.

Por lo anterior, este Sujeto Obligado, procede a integrar el presente documento de seguridad en cumplimiento a lo dispuesto por los artículos 32, 33, 34, 35, 37 y 38 de la Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados del Estado de Quintana Roo.

II. GLOSARIO

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

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

III. **Bloqueo:** 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 cancelación en la base de datos, archivo, registro, expediente o sistema de información que corresponda;

IV. **Comité de Transparencia:** Instancia a que se refiere el Capítulo III de la Ley de Transparencia y Acceso a la Información Pública del Estado de Quintana Roo;

V. **Consentimiento:** Manifestación de la voluntad libre, específica e informada del 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 al 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;

XII. **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 presente Ley y demás normatividad aplicable en la materia;

XIII. **Fuentes de acceso público:** Aquellas bases de datos, sistemas o archivos que por disposición de ley 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 por la Ley;

XIV. **Ley:** Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Quintana Roo;

XV. **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;

XVI. **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;

XVII. **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.

XVIII. **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.

XIX. **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 Quintana Roo, que decide y determina los fines, medios y demás cuestiones relacionadas con determinado tratamiento de datos personales;

XX. **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;

XXI. **Titular:** Persona física a quien corresponden los datos personales;

XXII. **Tratamiento:** Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos físicos o automatizados aplicados a los datos personales, relacionadas, 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.

III. NOMBRE DE LOS SISTEMAS DE TRATAMIENTO O BASE DE DATOS PERSONALES Y EL NOMBRE, CARGO Y ADSCRIPCIÓN DEL ADMINISTRADOR

Nombre de los sistemas de tratamiento o base de datos personales	Nombre, cargo y adscripción del administrador
1.- Administración de Recursos Humanos de la Consejería Jurídica del Poder Ejecutivo del Estado	Director de Administración y Finanzas: Lic. Danny Alejandro Durán Suárez

El objeto de esta base de datos o sistema de tratamiento es llevar un registro de todas las personas involucradas en trámites de contratación, ingreso, designación, pago de nómina, cumplimiento de obligaciones legales, administrativas, fiscales ante las autoridades correspondientes, integración de expedientes personales de cada uno de los servidores públicos prestadores de servicios profesionales y servicio social, con el fin de poder comunicarse, identificar y ubicar a los mimos, así como dar cumplimiento a las obligaciones establecidas en los distintos ordenamientos legales.

IV. FUNCIONES Y OBLIGACIONES DEL RESPONSABLE

Sistema de tratamiento y/o base de datos personales	Funciones y Obligaciones
Administración de Recursos Humanos	Funciones: • Tramitar ante la Secretaría de Finanzas y pLAneación todo lo relativo a nombramientos, remociones, licencias, incapacidades, renuncias, estímulos y recompensas, pensiones y jubilaciones de las y los servidores públicos de la Consejería Jurídica del Poder Ejecutivo. • Proponer a la Consejera o Consejero la celebración de convenios con instituciones educativas para allegarse de prestadores de servicio social de las carreras técnicas y profesionales que correspondan a las actividades de la Consejería, así como para apoyos en capacitación y proyectos afines a la misma. Obligaciones: • Coordinar que la información se encuentre actualizada y que se apliquen las medidas de seguridad de acceso a la misma.

V. INVENTARIO DE DATOS PERSONALES TRATADOS EN CADA SISTEMA DE TRATAMIENTO Y/O BASE DE DATOS PERSONALES

Nombre de los sistemas de tratamiento o base de datos personales	Categorías de datos personales	Datos Personales	Fundamento Legal
Administración de Recursos Humanos	**Datos de Identidad**	➢ Nombre Completo ➢ Domicilio Particular ➢ Teléfono Celular ➢ Registro Federal de Contribuyentes (RFC) ➢ Fotografía ➢ Edad	De conformidad con el numeral Tercero de los Lineamientos para la Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Quintana Roo
	Datos electrónicos	➢ Correo electrónico personal y oficial ➢ Firma electrónica	
	Datos laborales	➢ Nombramientos ➢ Capacitación ➢ Cargos o puestos desempeñados	
	Datos académicos	➢ Último grado de estudios ➢ Títulos ➢ Cédula profesional ➢ Constancias escolares	
	Datos de salud	➢ Incapacidades médicas	
	Datos afectivos y/o familiares	➢ Estado civil ➢ Número de hijos	
	Datos personales de naturaleza pública	➢ Correo electrónico institucional ➢ Información curricular ➢ Remuneración neta y bruta ➢ Cargo o puesto	

VI. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO Y/O BASES DE DATOS PERSONALES SEÑALANDO EL TIPO DE SOPORTE Y LAS CARACTERÍSTICAS DEL LUGAR DONDE SE RESGUARDAN

Nombre de los sistemas de tratamiento o base de datos personales	Tipo de Soporte	Características del lugar de resguardo	Programas en los que se utilizan los Datos Personales
	Físico: Documentos y Expedientes	Avenida Álvaro Obregón, número 401, Col, Centro, C.P. 77000. Chetumal Quintana Roo, México.	Paquetería office: Word y Excel
Administración de Recursos Humanos	**Electrónico:**	Computadora de escritorio tipo PC marca Ghia Frontier Slim, procesador INTEL Modelo Core 139100F Quad Core 3.60 GHZ/8GB/SSD/240GB/GT710/Win10Home. Monitor Led 19" VGA/VESA/Energy Star, número de serio 40752.	

VII. CONTROLES Y MECANISMOS DE SEGURIDAD PARA LAS TRANSFERENCIAS DE DATOS PERSONALES

Transmisiones mediante el traslado de soportes físicos.	➢ El envío se realiza a través del personal adscrito a la Dirección de Administración y Finanzas o mediante el personal autorizado por la o el Consejero Jurídico, previo oficio de comisión y/o permiso; ➢ Cuando se transfiere información que contenga datos personales y sea de carácter confidencial, esta se realiza en sobres sellados y se utiliza la leyenda de clasificación señalada en los Lineamientos Generales para la Clasificación y Desclasificación de la Información, así como para la Elaboración de las Versiones Públicas; ➢ La información sólo es entregada a los titulares de la información o a sus autorizados, previa acreditación con identificación oficial con fotografía; ➢ Toda entrega de información requiere acuse de recibo; y ➢ A partir de la aprobación del presente documento todas las transmisiones serán registradas en las bitácoras de transferencia del área respectiva.

Transmisiones mediante el traslado físico de soportes electrónicos	➢ El envío se realiza a través del personal adscrito a la Dirección de Administración y Finanzas o mediante el personal autorizado por la o el Consejero Jurídico, previo oficio de comisión y/o permiso; ➢ Cuando se transfiere información que contenga datos personales y sea de carácter confidencial, esta se realiza en sobres sellados y se utiliza la leyenda de clasificación señalada en los Lineamientos Generales para la Clasificación y Desclasificación de la Información, así como para la Elaboración de las Versiones Públicas; ➢ La información sólo es entregada a los titulares de la información o a sus autorizados, previa acreditación con identificación oficial con fotografía; ➢ Toda entrega de información requiere acuse de recibo; ➢ A partir de la aprobación del presente documento todas las transmisiones serán registradas en las bitácoras de transferencia de cada área; y ➢ A partir de la aprobación del presente documento todos los soportes electrónicos que sean transferidos y contengan información confidencial deberán estar cifrados.
Transmisiones mediante el traslado sobre redes electrónicas	En caso de ser necesario el envío se realiza a través del personal adscrito a la Dirección de Administración y Finanzas o mediante el personal autorizado por la o el Consejero Jurídico, únicamente a través de medios electrónicos institucionales

VIII. RESGUARDO DE LOS SOPORTES FÍSICOS Y/O ELECTRÓNICOS DE LOS DATOS PERSONALES

a) Resguardo físico

EQUIPO	BAJO RESGUARDO	CARGO	MARCA	MODELO	SERIE
DIRECCIÓN ADMINISTRATIVA					
Archivero Metálico con gavetas y llave.	Mtra. Diana May de la Cruz	**Jefa de Departamento de Recursos Humanos**	**N/A**	**N/A**	**N/A**

b) Resguardo electrónico

EQUIPO	BAJO RESGUARDO	CARGO	MARCA	MODELO	SERIE
DIRECCIÓN ADMINISTRATIVA					
PC de escritorio	Mtra. Diana May de la Cruz	Jefa de Departamento de Recursos Humanos	Ghia Frontier Slim Intel	Corel 39100f Quad Core	407252

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

Este Sujeto Obligado no requiere de bitácoras de acceso en soportes físicos ya que únicamente el personal autorizado de la Dirección de Administración y Finanzas tiene acceso a los expedientes físicos y sistemas de tratamiento o base de datos personales de esta Consejería Jurídica.

No obstante, es necesario contemplar nuevos formatos en los que se detalle la operación cotidiana y las posibles vulneraciones a la seguridad de los datos personales

De acuerdo con el artículo 40 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Quintana Roo, se consideran como vulneraciones de seguridad:

I. La pérdida o destrucción no autorizada;
II. El robo, extravío o copia no autorizada;
III. El uso, acceso o tratamiento no autorizado, o
IV. El daño, la alteración o modificación no autorizada.

En este sentido, las vulneraciones deberán ser reportadas dentro de una bitácora que describa, entre otros datos, la naturaleza del incidente, la fecha en que ocurrió, el motivo de la vulnerabilidad, los datos personales comprometidos, las acciones correctivas implementadas de forma inmediata y definitiva por mencionar algunos.

Bitácoras de acceso, operación cotidiana y vulneraciones a la Seguridad de los Datos Personales	
Fecha del incidente	
Nombre y cargo	
Área de adscripción	
Responsable del área	
Sistema de tratamiento o base de datos personales vulnerada	
Cantidad de titulares vulnerados	
Soporte de la información vulnerada	
Tipo de vulneración	
Tipo de dato personal afectado	
Nombre y firma de quien reporta	
Nombre y firma del administrador del sistema	

X. ANÁLISIS DE RIESGOS

De conformidad con los artículos 34, fracción IV, y 37, fracción III, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Quintana Roo, resulta necesario realizar el análisis de riesgo de los datos personales y de los recursos involucrados en su tratamiento, con la finalidad de identificar el nivel de riesgo que se tiene en la Institución, en relación con el tratamiento de datos personales, y poder implementar en consecuencia las medidas de seguridad que resulten necesarias.

El nivel de riesgo por tipo de datos es igual al beneficio que representa la información para un atacante, y para calcularlo se requieren dos elementos principalmente:

1. Tener el nivel de riesgo inherente de cada tipo de dato que se trate, y;
2. Calcular el volumen de titulares, cuantificando el número de personas de las que se traten datos personales.

Nivel de Protección básico: Datos de Identificación y Datos Laborales
Nivel de Protección medio: Datos patrimoniales; datos sobre procedimientos administrativos seguidos en forma de juicio o jurisdiccional; datos académicos y movimientos migratorios.
Nivel de Protección alto: Datos ideológicos, datos de salud, características personales, características físicas, vida sexual, origen étnico y racial.

Para tal efecto, se tomará como base de dicho análisis la Metodología de análisis de Riesgo BAA, propuesta por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI). En tal sentido, toda vez que en el presente documento de seguridad se han identificado previamente los diversos sistemas de tratamiento y/o bases de datos existentes en la Institución, y los datos personales que en ellos se tratan, se procede a determinar, conforme a la metodología citada, lo siguiente:

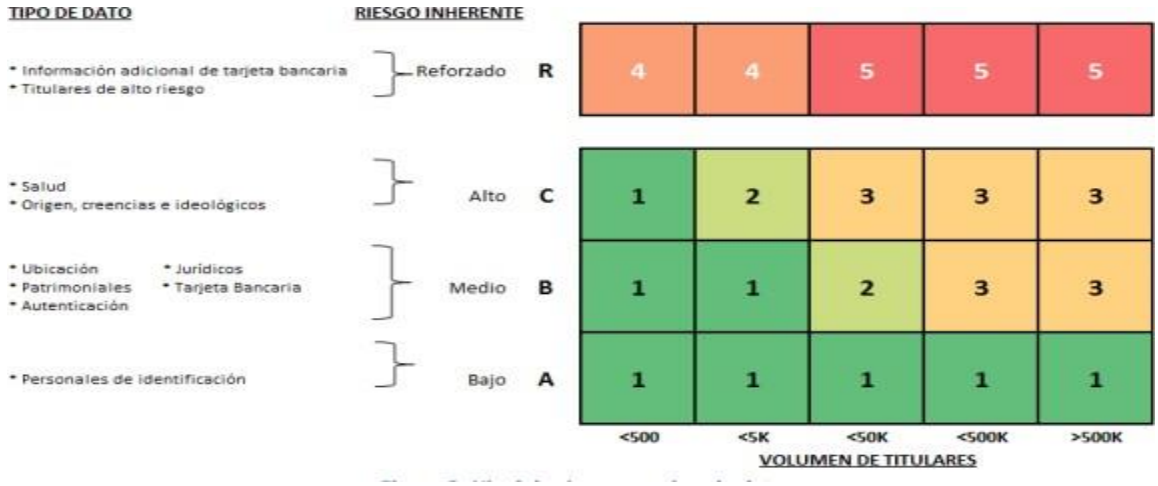
Primero. – El nivel de riesgo por tipo de dato (factor beneficio) resultado de:

1. El nivel de riesgo inherente por tipo de dato (conforme lo establece la metodología).
2. El volumen de titulares (cantidad de personas físicas sobre las cuales se tiene dicho dato)

Tipo de dato personal	Nivel de riesgo inherente	Volumen de titulares
Nombre Completo	**bajo**	**<500**
Teléfono celular	**bajo**	**<500**
Registro Federal de Contribuyente	**bajo**	**<500**
Cedula Profesional	**bajo**	**<500**
Correo Electrónico Personal	**bajo**	**<500**
Nombramientos	**bajo**	**<500**

El volumen de titulares se calcula acotando la cantidad de personas en un sistema de tratamiento de datos personales:

Toda vez que mediante la tabla anterior ha quedado establecido el nivel de riesgo inherente por cada tipo de dato y el volumen de titulares, se procede a identificar el nivel de riesgo por tipo de dato tratado en la Consejería Jurídica del Poder Ejecutivo del Estado de Quintana Roo, otorgándole a cada nivel de riesgo un valor numérico del 1 al 5, donde 1 es el nivel más bajo y el 5 el más alto, lo cual se ejemplifica de la en la siguiente tabla.



A continuación, se detallan los niveles mencionados:
Riesgo por tipo de dato Nivel 1, ocurre cuando:

- El nivel de riesgo inherente de los datos sea bajo, sin importar en número de personas
- El nivel de riesgo inherente sea medio y se tengan hasta cinco mil (5,000) personas
- El nivel de riesgo inherente sea alto y se tengan hasta quinientos (500) personas

De los datos proporcionados con anterioridad, se puede inferir lógicamente que el nivel de riesgo por tipo de datos (factor Beneficio) para la Consejería Jurídica del Poder Ejecutivo del Estado es igual a Riesgo por Tipo de Dato (el nivel que corresponda), conforme a la Metodología de análisis de Riesgo BAA.

Segundo. – El nivel de riesgo por la cantidad de accesos potenciales a los datos personales (factor accesibilidad)

Ejemplo:

Establecido el nivel de riesgo por tipo de dato, procede determinar el nivel por tipo de acceso, determinado por la cantidad de accesos potenciales a los datos personales que se pretenden proteger, es decir, definiendo cuántas personales tienen la posibilidad de acceder a la información en un intervalo de tiempo determinado, conforme a la siguiente tabla:

Accesibilidad (cantidad de acceso a los datos personales)
< 10
>10 < 100
>100 < 1,000
>1,000

De lo anterior, y toda vez que se conoce que la cantidad de personas que laboran actualmente en el área involucrada en el tratamiento de datos personales es menor a 10, resulta evidente que para la Consejería Jurídica del Poder Ejecutivo del Estado de Quintana Roo el nivel de riesgo por cantidad de accesos potenciales es bajo.

Tercero. – El nivel de riesgo por tipo de entorno (factor anonimidad).

Ejemplo:

El factor anonimidad representa el nivel de percepción que se tiene de que un atacante potencial provoque consecuencias negativas para la organización, en caso de acceder o hacer uso no autorizado de los datos personales que se tratan, determinándose en tal sentido el nivel de riesgo por el tipo de entorno, en el que, teniendo una escala del 1 al 5, en donde 1 implica anonimidad y 5 mayor anonimidad del atacante, entre más anónimo pueda ser un atacante, mayor confianza obtiene para intentar vulnerar la seguridad.

Entorno	Nivel de Anonimidad
Físico	**1**
Red Interna	**2**
Red inalámbrica	**3**
Red de Terceros	**4**
Internet	**5**

XI. 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 en base a las mejores prácticas.

A continuación, se enlistan algunos supuestos que pueden originar posibles vulneraciones a la seguridad de los datos personales que se resguardan:

- No contar con las medidas necesarias para garantizar el acceso restringido a los archivos donde se encuentren los datos personales de los Servidores Públicos.
- Permitir a todo servidor público o personas ajenas al sujeto obligado, el acceso a los expedientes que contienen datos personales, sin registros o bitácoras.
- Fallas técnicas en los equipos de cómputo en donde se encuentren las bases de datos.
- Diligencias inadecuadas, malas prácticas de los servidores públicos en relación a la confidencialidad que deben guardar sobre los datos personales que conozcan y traten debido al desempeño de sus funciones.

- Pérdida, robo o extravío de expedientes integrados con datos personales.
- Alteración de la información respecto a los datos personales.
- Susceptibilidad en redes o sistemas autorizados.

XII. GESTIÓN DE VULNERACIONES

La gestión de vulneraciones es un proceso en el que, una vez identificadas las brechas de seguridad, se plantea un esquema de prevención para evitar accesos no deseados a sistemas y datos confidenciales. Esto incluye trabajar de manera paralela con el desarrollo de políticas de seguridad, detención de activos, supervisión de perímetros y priorización de las amenazas.

Plan de respuesta:

- Restauración inmediata de la operatividad mediante los respaldos de los soportes electrónicos y versiones digitales de los soportes físicos.
- En caso de que la vulneración fuera resultado de la comisión de un delito realizar las denuncias correspondientes.
- Determinación de la magnitud de la afectación y elaboración de recomendaciones para los titulares.
- Elaboración de informe y propuesta de medidas correctivas a corto y mediano plazo por parte de la Dirección Administrativa.
- Notificación a titulares en un plazo de 72 horas que de forma significativa vea afectados sus derechos patrimoniales o morales.
- Llenado de la bitácora de vulneraciones conforme al artículo 59 de la Ley de Datos Personales en Posesión de Sujetos Obligados del Estado de Quintana Roo.

XIII. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

En términos del artículo 4 fracción XXVI de la Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados del Estado de Quintana Roo, las medidas de seguridad son un conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permiten garantizar la protección, confidencialidad, disponibilidad e integridad de los datos personales, sujetos a tratamiento al interior del responsable, y de los que se transfieran o remitan por diversas vías, a saber, las medidas de seguridad que actualmente se aplican son las siguientes:

A. Medidas de Seguridad Físicas

Para garantizar la seguridad física de las instalaciones, personas y equipos de la institución se cuenta con procedimientos de control y prevención ante amenazas al entorno físico de los datos y de los recursos involucrados en su tratamiento, los cuales se describen a continuación:

Medidas de Seguridad Físicas

Medida	Finalidad	Descripción
Seguridad privada en el edificio	▪ Prevenir el acceso no autorizado al perímetro de organización. ▪ Prevenir el daño o interferencia a las instalaciones. ▪ Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico	Las instalaciones son resguardadas por elementos de vigilancia privada las 24 horas del día.
Barda perimetral	▪ Prevenir el acceso no autorizado al perímetro de la organización. ▪ Prevenir el daño o interferencia a las instalaciones. ▪ Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico.	Las instalaciones cuentan con barda perimetral de aproximadamente de 6 metros de altura que cubre la totalidad de las instalaciones, y cuentan con un acceso principal
Acceso a la Dirección de Administración y Finanzas	▪ Prevenir el acceso no autorizado al perímetro de la organización. ▪ Prevenir el daño o interferencia a las instalaciones.	La Dirección de Administración y Finanzas cuenta con puertas de acceso con cerradura, las llaves se encuentran bajo resguardo del titular del área administrativa.

	▪ Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico.	Fuera del horario oficial de labores, salvo situaciones extraordinarias, la puerta de acceso al área donde se resguardan los expedientes físicos que contienen datos personales se deben de mantener cerradas bajo llave.
Seguridad física de equipos	▪ Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico	El equipo de cómputo se sitúa sobre una superficie fija, mesa de trabajo y escritorio, a una altura adecuada para evitar daños por estas. Los equipos de cómputo se ubican lejos de ventanas para evitar que se puedan mojar por fuertes lluvias. Tanto los equipos de cómputo (soportes electrónicos) como archiveros (soporte físicos) cuentan con el debido cuidado por parte del servidor público del cual se encuentra bajo resguardo

B. Medidas de Seguridad Técnicas

Para garantizar la seguridad técnica y operatividad de los recursos tecnológicos (hardware y software) involucrados en el tratamiento de datos personales se realizan e implementan las acciones y mecanismos siguientes:

Medidas de Seguridad Técnicas

Medida	Finalidad	Descripción
Usuarios y contraseñas	Prevenir que el acceso a los datos personales, así como a los recursos, sea por usuarios identificados y autorizados; Generar un esquema de privilegios para que el usuario lleve a cabo las actividades	Los equipos de cómputo asignados a cada servidor público para el desempeño de sus funciones, cuentan con contraseña de encendido y contraseña de usuario.

	que requiere con motivo de sus funciones.	
Software de Seguridad	Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware.	Todos los equipos de cómputo cuentan con programas antivirus bajo licencia. Los registros de renovación de licencia o cambio de software corren a cargo del área de informática
Mantenimientos de equipos	Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware	Realizar de manera periódica el mantenimiento preventivo o, en su caso, correctivo de los equipos de cómputo en los cuales se tratan datos personales. Se lleva una bitácora de tales acciones a cargo de la Dirección de la Información.

C. Medidas de Seguridad Administrativas

Para garantizar la seguridad administrativa de los datos personales en la gestión de los procesos 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 se toman las siguientes medidas:

Medidas de Seguridad Administrativas

Medida	Finalidad	Descripción
Capacitación general y particular	Sensibilizar y capacitar al personal en materia de protección de datos personales. Que el personal conozca y cumpla con los principios, deberes, derechos y demás obligaciones en la materia y las sanciones en caso de incumplimiento	Capacitaciones sobre aspectos generales de la ley en la materia.

Establecer 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.	Delimitar las actuaciones en la gestión de los procedimientos internos. Establecer los principios que rigen el actuar de los servidores públicos de la Consejería Jurídica del Poder Ejecutivo del Estado.	De acuerdo las Funciones establecidas en el Reglamento Interior de la Consejería Jurídica del Poder Ejecutivo del Estado y otras disposiciones normativas aplicables.

XIV. CONTROLES DE IDENTIFICACIÓN Y AUTENTIFICACIÓN

Los servidores públicos trabajadores de la Consejería Jurídica del Poder Ejecutivo del Estado de Quintana Roo, en todo momento deberán identificarse con el personal de seguridad privada de la Dependencia, quien llevará un registro de los ingresos y salidas de personas.

XV. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS PERSONALES

Es el procedimiento que se implementa cuando queremos tener resguardados nuestros datos o documentos en caso de que suceda algún imprevisto con nuestros sistemas informáticos, más precisamente con los discos duros, ya que estos son bastante delicados y son uno de los componentes informáticos con más alta probabilidad de presentar fallos.

Un respaldo de información bien organizado y estructurado nos permitiría volver a acceder a nuestros documentos para continuar trabajando con la mayor velocidad y eficiencia posibles, además de evitar que información importante se pierda, y con ella años de trabajo.

En este sentido, las normas de operación de respaldos contempladas se guían por lo siguiente:

- El respaldo de información se efectuará en discos duros.
- Los respaldos en el servidor se realizan en el site, de manera mensual; en caso de que no se pueda realizar el respaldo por algún problema con el servidor, se procederá a realizarlo en el día posterior inmediato.
- El respaldo correspondiente se realizará conteniendo la información del mes.

XVI. PLAN DE CONTINGENCIA

Este apartado tiene como finalidad prever un marco de actuación ante una situación de contingencia que ponga en riesgo los datos personales que resguarda esta Consejería Jurídica.

Clasificación de la Contingencia:

Según sea el tipo de la contingencia se le puede asignar un grado de afectación:

- **Grado 1:** Son las más bajas que van desde fallas eléctricas, fallas con la conexión de internet y que pueden ser resueltas por el mismo personal del organismo.

- **Grado 2:** Requiere tanto el apoyo del personal del Organismo, así como de personal externo (por ejemplo, en un incendio apoyo de bomberos y protección civil).

- **Grado 3:** Son contingencias que por su alcance pueden afectar severamente la operatividad del organismo y se requiere además del apoyo externo.

a. Unidad Interna de Protección.

Se conformará la Unidad Interna de Protección Civil esta será el primer contacto con los cuerpos de emergencia en las tareas de protección civil de la Consejería Jurídica y la máxima autoridad en la materia al momento de presentarse un alto riesgo, emergencia, siniestro o desastre, el cual tendrá las siguientes funciones:

- Coordinar las acciones de protección civil en la comisión ante situaciones de riesgos y emergencias.
- Elaborar y coordinar el programa interno de protección civil.
- Difusión del documento una vez aprobado.
- Integrar la unidad interna de protección civil de la Consejería Jurídica.
- Se debe contar con un responsable general quien guiará la implementación del mismo, así como la toma de las decisiones.
- Elaborar programas de actividades de capacitación y difusión.
- Identificar, analizar y evaluar riesgos internos y externos.
- Supervisar, elaborar y actualizar directorios de emergencias.
- Promover la capacitación respecto a la prevención, atención y recuperación de desastres para todo el personal involucrado

b. Medidas de prevención y conservación de archivos

- Espacios con luz natural y sin humedad.
- Los muebles de archivo deben garantizar la conservación de los documentos que guardan; los documentos deben guardar uniformidad.
- Evitar archivar documentación cerca de aparatos eléctricos, las instalaciones eléctricas deben estar en buenas condiciones.

- Los estantes de los archivos deben estar entre 10 y 15 cm del suelo (facilitan la limpieza y evita a su vez la acumulación de humedad y proliferación de plagas).
- Todos los equipos eléctricos deben quedar apagados y desconectados durante la noche o cuando no se utilicen.
- Se recomienda no colocar vasos con líquido que puedan derramarse fácilmente sobre los aparatos eléctricos.

c. Medidas Preventivas ante siniestros

- **Incendio:** Si detecta un incendio procure mantener la calma y repórtelo inmediatamente a la brigada de prevención y combate de incendios para que atiendan la emergencia conforme a la planificación.

Durante un incendio:

- Si el incendio es pequeño, se procurará apagarlo mediante un extintor.
- Si el fuego es de origen eléctrico no se deberá intentar apagarlo con agua.
- No abra puertas ni ventanas el fuego se extiende con el aire.
- Si el incendio no se puede controlar solicitar apoyo a los bomberos.
- No pierda tiempo buscando objetos personales y salga del inmueble lo antes posible.
- Si hay gas o humo humedezca un trapo cubriendo nariz y boca.
- Si su ropa se enciende; tírese al piso y ruede lentamente.

Después del incendio:

- Mantener suspendida la corriente eléctrica y del agua hasta que se revise el estado general del inmueble.
- Un técnico debe revisar las instalaciones de electricidad antes de utilizarlas nuevamente.

Resguardo de la información en caso de incendio:

- Respaldo de información en una zona segura de preferencia, donde el calor de un incendio no alcance los dispositivos, esto es en lugares cercanos a los extintores.
- Tener identificados los documentos con mayor valor para resguardarlos en una zona segura.

- **Inundaciones:** Para evitar pérdidas graves es importante realizar la revisión y reparación de ventanas y puertas, por donde podría filtrarse el agua de lluvia, así como impermeabilizar los techos en temporadas de lluvias para evitar filtraciones de agua.

Previamente:

- Evitar colocar expedientes y/o documentos directamente sobre el piso.
- Respetar, al menos, una altura de 10 a 15 cm de los archiveros.

- Colocar barreras para el agua (cubrir documentos de las goteras)
- Evacuar los documentos afectados hacía áreas ventiladas.
- Inmediatamente colocar papel secante en cada hoja de los expedientes.
- Si un documento en papel se moja en su totalidad se puede secar individualmente mediante ventilación del mismo.

Durante una inundación:

- Desconectar servicios de luz y agua.
- Mantenerse alejados de árboles y postes de luz.
- Evitar tocar o pisar cables eléctricos.
- Cubrir aparatos u objetos que puedan dañarse con el agua.

Después de la inundación:

- Expulsar el agua mediante esponjas, baldes, recogedores, en el caso de no contar con bomba de motor de combustión.
- Cerciorarse de que los aparatos eléctricos estén secos antes de utilizarlos nuevamente.
- Desinfectar las áreas afectadas pisos, muros y mobiliario rescatable, con agua, jabón y cloro para evitar enfermedades.
- Ventilar las áreas afectadas después de la inundación.
- Identificar documentos dañados con la inundación y proceder a aplicar medidas para recuperarlo.
- Reportar lo que se dañó con el paso de la inundación.

- **Amenazas informáticas:** Ante un evento informático los pasos a seguir para mantener la seguridad de la información, son los siguientes:

  - Cambiar contraseñas.
  - Las contraseñas no deben contener información personal como nombre real, nombre de usuario, fechas de nacimiento o incluso el nombre institucional.
  - Deben ser distintas a otras contraseñas.

Para la atención ante una situación de emergencia de este tipo se utilizarán los siguientes elementos:

- Equipos contra incendio: En las instalaciones se dispondrán y ubicarán extintores en un lugar visible y de fácil acceso.
- Se deberá tener acceso al botiquín para realizar tratamientos de primeros auxilios.
- Mientras se está conectado a internet el atacante tendrá acceso a los archivos e información guardados en la computadora vulnerada, por lo que se recomienda desconectar el cable de la red lo antes posible.

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

Las técnicas de borrado seguro implementadas por la Consejería Jurídica, buscan que no sea posible recuperar la información, tanto física como electrónica, y evitar que personas no autorizadas puedan tener acceso a los datos. Se contemplan métodos físicos basados en la destrucción de los medios de almacenamiento, así como métodos lógicos basados en la limpieza de los datos almacenados.

Desmagnetización

La desmonetización 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, como, 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 para evitar la recuperación posterior de los datos que almacena. Existen diferentes tipos de técnicas y procedimientos para la destrucción de medios de almacenamiento: desintegración, pulverización, fusión e incineración: son métodos diseñados para destruir por completo los medios de almacenamiento. Los cuales consisten en:

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 que no pueden ser reconstruidos.

Destrucción de los medios de almacenamiento electrónicos mediante desintegración: Los medios ópticos de almacenamiento (CD, DVD, magneto-ópticos) deben ser destruidos por pulverización, trituración de corte transversal o incineración. Cuando el material se desintegra o desmenuza, 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.

XVIII. PLAN DE TRABAJO

Una vez realizados el análisis de riesgos y el análisis de brecha, la unidad administrativa responsable elaborará por cada sistema, un plan de trabajo para la implementación de las medidas de seguridad faltantes.

XIX. PROGRAMA GENERAL DE CAPACITACIÓN

Se establecerá al principio de cada ejercicio el Programa anual de capacitación, que contemplará las necesidades de la unidad administrativa responsable del tratamiento de datos personales.