ANEXO I

POLÍTICAS INTERNAS GENERALES PARA LA GESTIÓN Y TRATAMIENTO DE DATOS PERSONALES EN EL SUJETO OBLIGADO, DENOMINADO: COORDINACIÓN GENERAL ESTRATÉGICA DE SEGURIDAD.

ANTECEDENTES.

PRIMERO.- Que el artículo 6o de la Constitución Política de los Estados Unidos Mexicanos establece toda persona tiene derecho al libre acceso a información plural y oportuna, así como al de buscar, recibir y difundir información e ideas de toda índole por cualquier medio de expresión. De la misma forma, que en principio toda la información en posesión de cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, así como de cualquier persona física, moral o sindicato que reciba y ejerza recursos públicos o realice actos de autoridad en el ámbito federal, estatal y municipal, es pública y sólo podrá ser reservada temporalmente por razones de interés público y seguridad nacional, en los términos que fijen las leyes.

Los sujetos obligados deberán documentar todo acto que derive del ejercicio de sus facultades, competencias o funciones, la ley determinará los supuestos específicos bajo los cuales procederá la declaración de inexistencia de la información.

SEGUNDO.- Que las bases y principios que rigen este derecho fundamental, establecidas en el apartado A del citado numeral, precisan que la información que se refiere a la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes; en esta vertiente, precisa que la Ley Reglamentaria establecerá aquella información que se considere reservada y confidencial. En la interpretación de este derecho deberá prevalecer el principio de máxima publicidad. Los sujetos obligados deberán documentar todo acto que derive del ejercicio de sus facultades, competencias o funciones, la ley determinará los supuestos específicos bajo los cuales procederá la declaración de inexistencia de la información; por lo que la información que se refiere a la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes. Del mismo modo; refiere que la inobservancia a las disposiciones en materia de acceso a la información pública será sancionada en los términos que dispongan las leyes.

TERCERO.- Que el artículo 16 segundo párrafo de la misma Constitución Política de los Estados Unidos Mexicanos, establece que ninguna persona puede ser molestada en su persona, familia, domicilio, papeles o posesiones, sino en virtud de mandamiento escrito de la autoridad competente, que funde y motive la causa legal del procedimiento. De igual manera, 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 rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud pública o para proteger los derechos de terceros.

CUARTO.- Que el artículo 4° de la Constitución Política del Estado de Jalisco, señala que toda persona que se encuentre en territorio Jalisciense gozará de los derechos y garantías que la misma establece, siendo una obligación fundamental de las autoridades salvaguardar su cumplimiento. De igual manera, que todas las autoridades, en el ámbito de sus competencias, deberán promover, respetar, proteger y garantizar los derechos humanos, de conformidad con los principios de universalidad, interdependencia, indivisibilidad y progresividad.

Por otro lado, establece que el derecho a la información pública tendrá como fundamento la transparencia y la rendición de cuentas por parte de las autoridades, la información veraz y oportuna, la protección de los datos personales en posesión de los sujetos obligados.

QUINTO.- Que la Ley General de Transparencia y Acceso a la Información Pública, publicada en el Diario Oficial de la Federación el día 04 cuatro de mayo de 2015 dos mil quince, es de orden público y de observancia general en toda la República Mexicana, reglamentaria del artículo 6o de la Constitución Política de los Estados Unidos Mexicanos en materia de transparencia y rendición de cuentas; tiene aplicación de manera supletoria al orden jurídico de esta entidad federativa, de acuerdo con lo que dispone el numeral 7° en el punto 1, fracción I de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios; la cual tiene como principal objetivo establecer las bases mínimas que regirán los procedimientos para garantizar el ejercicio del derecho de acceso a la información en el país.

SEXTO.- Que el Congreso General de los Estados Unidos Mexicanos, DECRETA: Se expide **Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados,** publicado en el Diario Oficial el día 26 veintiséis de Enero del año 2017 dos mil diecisiete, la cual es de orden público y de observancia general en toda la República, reglamentaria de los artículos 6o., Base A y 16, segundo párrafo, de la Constitución Política de los Estados Unidos Mexicanos, en materia de protección de datos personales en posesión de sujetos obligados y que tiene por objeto establecer las bases, principios y procedimientos para garantizar el derecho que tiene toda persona a la protección de sus datos personales, en posesión de sujetos obligados, en el ámbito federal, estatal y municipal, cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos.

SÉPTIMO.- Que la vigente Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios, es el ordenamiento reglamentario de los artículos 6o apartado A y 16 párrafo segundo de la Constitución Política de los Estados Unidos Mexicanos, así como el artículo 9 de la Constitución Política del Estado de Jalisco, el cual tiene por objeto principal garantizar y hacer efectivo el ejercicio del derecho humano que permite solicitar, consultar, recibir, difundir, reproducir y publicar aquella información pública en poder de los sujetos obligados, así como proteger los datos personales en posesión de estos, como información confidencial de conformidad con las disposiciones legales aplicables; entre otras.

OCTAVO.- Que la Ley en vigor denominada Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios; publicada mediante el Decreto 26420/LXI/17, a través del Periódico Oficial: "El Estado de Jalisco", el día miércoles 26 veintiséis de julio del año 2017 dos mil diecisiete, siendo ésta de orden público y de observancia general en todo el territorio del Estado de Jalisco, reglamentaria de los artículos 6 base A y 16 párrafo segundo de la Constitución Política de los Estados Unidos Mexicanos, así como el artículo 9 de la Constitución Política del Estado de Jalisco, en materia de protección de datos personales en posesión de sujetos obligados.

NOVENO.- Que fue aprobado por el Congreso del Estado de Jalisco, el Decreto número 27213/LXIV18 mediante el cual se abroga la Ley Orgánica del Poder Ejecutivo y crea la Nueva Ley Orgánica del Poder Ejecutivo del Estado de Jalisco; así como el decreto número 27214/LXII/18; en donde se abroga la actual Ley Orgánica de la Fiscalía General del Estado de Jalisco, y se expide la Ley Orgánica de la Fiscalía del Estado de Jalisco; ambos ordenamientos del Estado de Jalisco, expedidos por el Congreso del Estado, mismas que se publicaron en el Periódico Oficial "El Estado de Jalisco" el día miércoles 5 cinco de Diciembre del año 2018 dos mil dieciocho; teniendo vigencia los mismos a partir del día 06 seis de Diciembre de 2018 dos mil dieciocho; por lo que conforme a los numerales 7.1 fracciones II y III, 11 puntos 1 y 2 fracción 1; 13, 16.1 fracción XV y 31 de la vigente Ley Orgánica del Poder Ejecutivo del Estado de Jalisco, en donde se enlistan las facultades y atribuciones de dependencias que integran la Administración Pública Centralizada; de igual forma es de considerarse las últimas reformas a la Ley del Sistema de Seguridad Pública para el Estado de Jalisco aprobadas mediante **DECRETO 27884/LXII/20,** publicado en el Periódico Oficial "El Estado de Jalisco" el día martes 21 veintiuno de Abril del año 2020 dos mil veinte.

DÉCIMO.- Este Sujeto Obligado Coordinación General Estratégica de Seguridad emitió el acuerdo mediante el cual se Constituye el Comité y la Unidad de Transparencia de la Coordinación General Estratégica de Seguridad, de conformidad a lo establecido en los numerales 7.1 fracciones II y III, 11 puntos 1 y 2 fracción 1; 13, 16.1 fracción XV y 31 de la vigente Ley Orgánica del Poder Ejecutivo del Estado de Jalisco; para que con las formalidades legales exigidas se atienda lo ordenado en el marco jurídico expresado en el presente Acuerdo, y cumplan con las atribuciones y obligaciones que la Ley de la materia impone, así como todas aquellas inherentes que se desprendan de ese u otros ordenamientos jurídicos, para el debido cumplimiento de las mismas.

DÉCIMO PRIMERO.- Que el actual Instituto de Transparencia, Información Pública y Protección de Datos Personales del Estado de Jalisco, es un Organismo Público autónomo, encargado principalmente de promover la transparencia, garantizar el acceso a la información pública de libre acceso y proteger la información pública reservada; así como garantizar el ejercicio del derecho a la protección de datos personales en posesión de sujetos obligados.

DÉCIMO SEGUNDO.- Con fundamento en el numeral 32, fracción I y 33, así como demás disposiciones del Título Segundo, Capitulo II de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios, el sujeto obligado responsable Coordinación General Estratégica de Seguridad del Estado de Jalisco para la gestión y tratamiento de datos personales.

OBJETIVO.

Las presentes políticas tienen por objeto de establecer y regular los procedimientos internos para la gestión y tratamiento de datos personales en este Sujeto Obligado, denominado: Coordinación General Estratégica de Seguridad, de conformidad con lo ordenado por los artículos 32, párrafo 1, fracción I y 33 de Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios, atendiendo a la obligación de esta Dependencia de garantizar la seguridad y el derecho a la protección de datos personales, así como reducir el número de probables vulneraciones a datos personales en posesión de este Sujeto Obligado Responsable.

OBLIGACIONES GENERALES PARA LAS DEPENDENCIAS, DIRECCIONES Y/O ÁREAS DEL SUJETO OBLIGADO COORDINACION GENERAL ESTRATEGICA DE SEGURIDAD.

1.- Seleccionar a un servidor público y/o elemento operativo que se encargue de los aspectos de transparencia y protección de datos personales.

La persona elegida deberá contar con habilidades y capacidades adecuadas en la materia y dedicarse a las tareas de transparencia y protección de datos personales; ya que el rol exige atención, dedicación, interés y conocimientos especializados.

La persona designada como enlace, deberá estar en contacto constante con la Unidad de Transparencia de la Coordinación General Estratégica de Seguridad, con el fin de atender y dar trámite a las solicitudes de acceso a la información pública, así como las solicitudes de ejercicio de los derechos ARCO, así como coadyuvar con la Unidad de Transparencia para efectos de publicación de información fundamental.

Para efectos de lograr la especialización del personal del sujeto obligado, es importante que dicha persona se capacite en las formaciones que pudiera llegar a ofrecer la citada Unidad de Transparencia, la Coordinación General de Transparencia del Poder Ejecutivo, institucionales de educación u órganos garantes en materia de transparencia y protección de datos personales.

2.- Crear una cultura consciente de la transparencia, así como de la seguridad y la protección de información.

Se deberá promover y asistir a sesiones de concientización y sensibilización, así como los foros, conferencias y programas educativos en la materia para lograr este objetivo. La Unidad de Transparencia de la Coordinación General Estratégica de Seguridad será la encargada de coordinar, participar o desarrollar dichas capacitaciones, así como bajo la dirección de la Coordinación General de Transparencia del Gobierno del Estado de Jalisco.

3.- Buscar recursos disponibles.

El servidor público y/o elemento operativo, que sea designada como Enlace, comenzará a identificar algunos recursos tangibles disponibles, tales como presupuesto o personal administrativo a su cargo. Además debe considerarse las áreas o unidades administrativas de la Dependencia que puedan ayudar al Enlace, como las áreas de tecnologías de la información, recursos humanos, de finanzas, de servicios generales; a lo que es esencial que la persona que funge como Enlace deberá conocer la organización y los procesos internos del flujo de trabajo; así como identificar las tecnologías disponibles en cada área o dirección, las cuales pueden ser plataformas institucionales para compartir archivos, antivirus, plataformas en línea, etc.

4.- Cumplir con las presentes políticas y las normas oficiales en materia de transparencia, de seguridad y protección de información, así como de archivos.

El servidor público y/o elemento operativo, que sea designada como Enlace ante la Unidad de Transparencia del Sujeto Obligado, deberá recabar, analizar y conocer la documentación legal disponible, tales como las presentes políticas, leyes, reglamentos, lineamientos y demás aplicable para su estudio y aplicables en la materia.

En caso de duda, el enlace podrá establecer comunicación con la Unidad de Transparencia de la Coordinación General Estratégica de Seguridad, o en su caso con sus áreas jurídicas o su homologo de la Coordinación General Estratégica de Seguridad, Secretaría de Seguridad, Secretariado Ejecutivo del Consejo Estatal de Seguridad Pública de Jalisco, Consejo Ciudadano de Seguridad y del Consejo de la Coordinación para la Implementación del Nuevo Sistema de Justicia Penal para el Estado de Jalisco.

ACCIONES PARA RESTAURAR LA DISPONIBILIDAD Y EL ACCESO A LOS DATOS PERSONALES DE MANERA OPORTUNA EN CASO DE UN INCIDENTE FÍSICO O TÉCNICO.

Es importante contar con seguridad relacionada con respaldos que permitan garantizar la disponibilidad de la información confidencial cuando se encuentre en medio magnéticos o digitales, en la medida de lo posible, se realizará una digitalización completa de la información confidencial o reservada, única y exclusivamente para su respaldo y el almacenamiento en discos duros, no siendo viable el uso de otras herramientas electrónicas portátiles en donde puedan extraer información de esa índole.

Se deberá repetir con cierta periodicidad las copias en los discos duros, para probar que continúa la información disponible, así como para incluir en dichas copias la nueva información que se haya generado.

Cada Dirección o área deberá gestionar programas de capacitación respecto al uso de equipos de cómputo, el uso e instalación de antivirus y actualización de software o cualquier otra herramienta tecnológica que permita garantizar el debido resguardo de información confidencial y reservada.

Coordinación
de Seguridad
GOBIERNO DE JALISCO

MEDIDAS CORRECTIVAS EN CASO DE IDENTIFICAR UNA VULNERACIÓN O INCIDENTE.

De manera previa, la Dirección o área informe a la Unidad de Transparencia de la Coordinación General Estratégica de Seguridad, sobre una vulneración o incidente, resulta sustancial que se identifiquen una serie de conceptos interrelacionados para tener un mejor contexto de la situación; para ello habrá que identificar cada unidad administrativa qué son activos, amenazas, vulneración, riesgo e incidente.

En el caso de activos, es todo aquel elemento de valor para una organización, involucrado en el tratamiento de datos personales, por ejemplo, en el caso de este sujeto obligado responsable podría ser una base de datos de empleados, elementos de seguridad en el estado, relación de vehículos con funciones de patrullas, personas detenidas, equipos de cómputos, correos electrónicos institucionales, etc.

Lo activos son susceptibles a amenazas, es decir a factores externos que tienen el potencial de dañarlos, desde un desperfecto de origen técnico hasta un acceso por parte de un persona que no tenga autorización para ello. Mientras que para que una amenaza tenga efecto, requiere explotar una vulnerabilidad, debilidad o falla propia de un activo, y cuando ese supuesto se pudiera materializar ocurre un incidente de inseguridad.

A la postre se precisan de manera enunciativa, más no limitativa algunos incidentes de de seguridad:

CATEGORIA	EJEMPLO
Desastre Natural	Terremoto, erupción de un volcán, tsunami, huracán, etc.
Inestabilidad Social	Huelgas, terrorismo, guerra, atentado.
Daño físico (accidental o meditado)	Incendio, inundación, malas condiciones ambiental (contaminación, polvo, corrosión, congelamiento) radiaci o pulso electromagnético, destrucción parcial de medi de almacenamiento físico o electrónico.
Falla técnica	Fallas de hardware, mal funcionamiento del softwa sobrecarga o saturación en el uso de los sistemas, falta mantenimiento.
Software malicioso	Diferentes categorías de software malicioso (malwa como virus, troyanos, software de acceso y control remo (RAT, por sus siglas en inglés) Ransomware.
Ataques técnicos	Explotación de vulnerabilidades de la configuración, protocolos o programas, normalmente a fuerza. Escaneo de redes, utilización de puertas traseras en software, intentos de acceso no autorizado, inferencia contraseñas, ataques de denegación de servicios.
Incumplimiento de las reglas o políticas (accidental o deliberado)	Uso no autorizado de activos, uso de activos autorizad pero para finalidades no autorizadas, uso software, o dispositivos no permitidos, instalación programas o aplicaciones no autorizadas o ilegales, co o sustracción de documentos o información no autorizad
Información dañada	Sobre escritura accidental, error de captura almacenamiento.
Intercepción de información	Espionaje, intervención de comunicaciones, ingenie social, robo, pérdida o extravío de información.
Divulgación de contenido perjudicial	Difusión en medios masivos de comunicación contenido ilegal, malicioso, abusivo o que pueda dañar derechos morales o patrimoniales de las personas.

Jalisco
GOBIERNO DEL ESTADO

En relación a lo anterior, es de enfatizar además tomar en consideración las vulneraciones de seguridad, las cuales pueden consistir en:

a) La pérdida o destrucción no autorizada de la información;

b) El robo, extravío o copia no autorizada de la información;

c) El uso, acceso o tratamiento no autorizado de la información; y

d) El daño, la alteración o modificación no autorizada de la información.

Una vez identificado lo anterior, conforme lo señala el artículo 39 de la Ley aplicable en la materia; la dirección o área, a través de su titular deberá general una bitácora que contendrá al menos lo siguiente:

1. Información confidencial comprometida, dañada o vulnerada.

2. La fecha en la que ocurrió la vulneración;

3. El motivo de la vulneración. Por ejemplo, archivos dañados por humedad;

4. Las acciones correctivas implementadas de forma inmediata y definitiva.

Por ejemplo, en el caso de la inundación, recuperar el acervo documental, separar las hojas con el debido cuidado, dejar secar bajo la sombra utilizando ventiladores que no generen humedad.

Una vez actualizada cualquiera de las hipótesis de riesgo ya señalados con anterioridad, deberá notificarse a la Unidad de Transparencia de la Coordinación General Estratégica de Seguridad, a más tardar el día hábil siguiente de que se cometa una vulneración o incidente, señalando lo siguiente:

1.- La naturaleza del incidente.
Por ejemplo, desastre natural, concerniente a una inundación;
2.- Los datos personales comprometidos.
Por ejemplo, identificativos: concernientes a nombres, domicilios, teléfonos particulares de servidores públicos y/o elementos operativos, etc.;
3.- Las recomendaciones y medidas que el titular de los datos personales puede adoptar para proteger sus intereses;
4. Las acciones correctivas realizadas de forma inmediata; y,
5. Los medios donde el titular de los datos personales puede obtener más información al respecto.

Cuando ocurre una vulneración a la seguridad de los datos personales, el Enlace del área o Dirección, en coordinación con la Unidad de Transparencia de la Coordinación General Estratégica de Seguridad y el Titular del Sujeto Obligado responsable deberá analizar las causas por las cuáles se presentó e implementar un plan de trabajo, identificando las acciones preventivas y correctivas para adecuar las medidas de seguridad y el tratamiento de los datos personales, si fuera el caso, a efecto de evitar que la vulneración se repita.
Por ejemplo: resguardar los documentos en cajas de plástico, colocarlas en lugares altos para evitar que se vuelvan a dañar o incluso mudarlos de lugar a un piso alto.

En caso de que se determine omisiones en la aplicación de la normatividad y las presentes Políticas Generales, se deberá conforme a derecho corresponda, pudiendo ser desde un apercibimiento al área o dirección, debiendo dar vista al órgano de control interno o en su caso al área de asuntos

internos; y en su caso si así se requiere proceder a la denuncia oportuna conforme la Ley aplicable en la materia.

PROCESO PARA EVALUAR PERIÓDICAMENTE LAS POLÍTICAS, A EFECTO DE MANTENER SU EFICACIA.

1.- La Unidad de Transparencia de la Coordinación General Estratégica de Seguridad, desarrollará campañas de concientización y sensibilización respecto de las presentes políticas generales, debiendo remitir las mismas a cada Dirección para su debida observancia.

2.- El servidor público y/o elemento operativo designado como Enlace de cada una de las Direcciones o Áreas, deberán revisar periódicamente que esté resultando positiva la implementación de la normativa interna en materia de protección de datos personales y seguridad de la información, en caso de que dicha hipótesis no se actualice, deberá hacerlo saber a través de su Director a la Unidad de Transparencia del Sujeto Obligado responsable.

3.- Todas las Direcciones o Áreas deberá dar cumplimiento a las nuevas disposiciones normativas, aquí determinadas de manera permanente y apegada a la normatividad aplicable.