Coordinación de Seguridad
GOBIERNO DE JALISCO

DOCUMENTO DE SEGURIDAD

COORDINACIÓN GENERAL ESTRATÉGICA DE SEGURIDAD

Contenido

I. INTRODUCCIÓN

Con fecha 5 de diciembre del año 2018, se abroga la Ley Orgánica del Poder Ejecutivo del Estado de Jalisco, mediante decreto número 27213/LXII/18, expedido por el Congreso del Estado en el Periódico Oficial "El Estado de Jalisco", y se expide la nueva "Ley Orgánica del Poder Ejecutivo del Estado de Jalisco" donde se crea la Coordinación General Estratégica de Seguridad, así como la Secretaría de Seguridad sectorizada a la misma, y mediante el acuerdo respectivo se concentra la Unidad de Transparencia de la Coordinación General Estratégica de Seguridad, así como se crea el Comité de Transparencia de la Coordinación General Estratégica de Seguridad.

Es de considerarse que en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios se establecen las bases, principios, procedimientos y tratamiento que permiten garantizar la protección de datos personales de los ciudadanos en posesión de la Coordinación General Estratégica de Seguridad.

Teniendo como base dicha normatividad, y de conformidad con sus artículos 3 fracción XIV, 30 al 44 y a la Guía para Elaborar un Documento de Seguridad, emitida por el Instituto de Transparencia, Información Pública y Protección de Datos Personales del Estado de Jalisco, se crea el presente documento de seguridad.

Desde la creación de este Sujeto Obligado se empezó a trabajar en el cumplimiento de las obligaciones establecidas de la Ley en referencia, en conjunto con los enlaces que se tiene en cada área generadora de información, se realizaron acciones que tuvieron como finalidad la creación de este documento.

De lo anterior derivó la elaboración de un listado de bases de datos tanto físicas como electrónicas donde se contienen datos personales que nos permitió identificar información en esa materia que son sometidos a tratamiento por cada área de la Coordinación General Estratégica de Seguridad.

Este documento permitió identificar los trámites donde se recaban y se realiza el tratamiento de datos personales para la creación de los sistemas de tratamiento de datos personales, así como obtener información valiosa para la elaboración de cada una de las partes de este documento, con el objetivo de propiciar la protección de los datos personales de la forma más completa y clara posible, ello encaminado a lograr el adecuado tratamiento de los datos personales.

El presente documento se guía por los principios, y conceptos que establece Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios.

II. FUNDAMENTACIÓN

Art. 3, fracción IX de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios, 7 fracción II y III, 11 punto 1 y 2 fracción I; 13, 16 punto 1 fracción XV y 31 de la vigente Ley Orgánica del Poder Ejecutivo del Estado de Jalisco, artículos 12, 13, 14 y 15 del Reglamento Interno de la Coordinación General Estratégica de Seguridad del Estado de Jalisco. Constitución Política de los Estados Unidos Mexicanos, Artículo 6º apartado A fracción II y 16 párrafo segundo. Artículos 7, 20 al 23 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios. Lineamientos Generales para la Protección de la Información Confidencial y Reservada que deberán observar los Sujetos Obligados previstos en la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios. Ley del Procedimiento Administrativo del Estado de Jalisco, de manera supletoria.

Código de Procedimientos Civiles del Estado de Jalisco, 40 fracciones I, II, y XXI, 122 de la Ley General del Sistema Nacional de Seguridad Pública, así como también en base a los derechos de personalidad consagrados en el Código Civil del Estado de Jalisco 24, 25, 28 fracciones V y VIII, 30, 40 bis 3, 40 bis 9 y 60.

III. DE LOS SISTEMAS DE TRATAMIENTO

SOLICITUDES DE ACCESO A LA INFORMACIÓN, DERECHOS ARCO Y RECURSOS DE REVISIÓN	
Datos de identificación:	
Fecha de Elaboración:	16 de agosto de 2021
Sujeto Obligado:	Coordinación General Estratégica de Seguridad
Unidad Administrativa Responsable:	Unidad de Transparencia de la Coordinación General Estratégica de Seguridad
Nombre y Cargo del Responsable:	Mtro. Javier Sosa Pérez Maldonado Director de la Unidad de Transparencia
Contenido del Sistema:	
Finalidad de sistemas y los usos previstos.	Tener un registro certero y continuo de las solicitudes de acceso a la información y de derechos ARCO que se presentan ante este Sujeto Obligado, así como de mantener datos sensibles ya sean del solicitante o que formen parte de respuestas, dentro de sus respectivos expedientes.
Las personas o grupos de personas sobre las cuales se obtienen los datos.	Solicitantes de información que pueden ser ciudadanos, periodistas, personal administrativo y operativo de la Secretaría de Seguridad.
Procedimiento de recolección	Formato Físico o por comparecencia, así como por medio del sistema de recepción de solicitudes llamado INFOMEX. También pueden ser recolectados por parte de las respuestas que brindan las áreas ya sea por medio de oficio o por correo electrónico.
Tipo de soporte en donde se contienen los datos personales:	Físico y electrónico.
Medidas de Seguridad:	Electrónico: Los archivos electrónicos se encuentran resguardados en la red común, la cual es gestionada por la Dirección de Tecnologías de Información y Telecomunicaciones, misma que cuenta con acceso a la mencionada red y realiza respaldos periódicos de la información. La Unidad de Transparencia actualmente cuenta con 13 ordenadores y cada uno de ellos posee para su acceso el mecanismo de seguridad de clave de usuario y contraseña. Físico: Los expedientes se tienen identificados con un número de control interno y resguardados en los cajones de los archiveros. Los archiveros que contienen los expedientes se encuentran dentro de la oficina designada a la unidad de transparencia,

	la cual cuenta con chapa y llave, manteniéndose cerrada cuando la unidad no se encuentra en funciones. Se cuenta además con un área de archivo, la cual se encuentra ubicada en el piso 9 del edificio sede de esta oficina. El área de archivo cuenta con chapa y su respectiva llave, la cual es resguardada y controlada por el propio titular de la unidad. Administrativo: Existe una sola llave dl almacén, misma que es resguardada únicamente por el titular del área.
Resguardo de los Soportes Físicos y/o electrónicos:	Resguardados en archiveros y en la red común. A esta red sólo tiene acceso el personal que labora en la Unidad de Transparencia y personal del área de informática a razón de que son ellos quienes la gestionan.
Estructura básica del sistema y la descripción de los tipos de datos incluidos:	
Área:	Unidad de Transparencia
Responsable y Administradores:	Director de la Unidad de Transparencia, Mtro. Javier Sosa Pérez Maldonado
Cargo:	Director de la Unidad de Transparencia
Domicilio:	Avenida 16 de Septiembre No. 400, esquina Libertad, Zona Centro, Guadalajara Jalisco.
Teléfono:	36687971 extensión 17971 y 17931
Correo electrónico:	transparencia.cges@jalisco.gob.mx
Administradores:	
Nombre:	Adriana Alejandra López Robles
Área:	Unidad de Transparencia
Cargo:	Jurídico Especializado
Nombre:	Alejandro Magallanes Ávila
Área:	Unidad de Transparencia
Cargo:	Jefe de Protección de Datos Personales de la Coordinación de Gabinete de Seguridad Pública
Nombre:	Alma Rocío Ayala Alejandre
Área:	Unidad de Transparencia
Cargo:	Jefe de Portal y Plataforma Nacional de Transparencia de la Coordinación de Gabinete de Seguridad Pública
Nombre:	Edson Roberto Reyes Cárdenas

Área:	Unidad de Transparencia
Cargo:	PERITO A
Nombre:	Sandra Edith de la Torre Fernández
Área:	Unidad de Transparencia
Cargo:	Auxiliar de Acceso a la Información de la Coordinación de Gabinete de Seguridad Pública
Nombre:	Sandra Herrera López
Área:	Unidad de Transparencia
Cargo:	Auxiliar de Acceso a la Información de la Coordinación de Gabinete de Seguridad Pública
Nombre:	Frida Fabiola Reyes Dávila
Área:	Unidad de Transparencia
Cargo:	Auxiliar de Acceso a la Información de la Coordinación de Gabinete de Seguridad Pública
Nombre:	José Luis Huerta Vázquez
Área:	Unidad de Transparencia
Cargo:	Auxiliar de Acceso a la Información de la Coordinación de Gabinete de Seguridad Pública
Nombre:	Néstor Gerardo Pérez Bravo
Área:	Unidad de Transparencia
Cargo:	Auxiliar del Portal Y Plataforma de la Coordinación del Gabinete de Gestión de Territorio C
Nombre:	Nancy Elizabeth Chávez Castro
Área:	Unidad de Transparencia
Cargo:	Coordinador de Planeación Seguimiento Y Evaluación
Nombre:	Enrique Javier Villanueva Villanueva
Área:	Unidad de Transparencia
Cargo:	Recepcionista
Nombre:	Juan Francisco Cuevas González

Área:	Unidad de Transparencia
Cargo:	Analista A
Funciones y obligaciones:	**REGLAMENTO DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN PÚBLICA Y PROTECCIÓN DE DATOS PERSONALES DE LA ADMINISTRACIÓN PÚBLICA CENTRALIZADA DEL ESTADO DE JALISCO.** I. Proporcionar la información pública que su área genere, posea o administre, como consecuencia del ejercicio de sus facultades, atribuciones o el cumplimiento de sus obligaciones y, en su caso, la versión pública de la misma, cuando le sea requerida para dar debido seguimiento y cumplimiento a las solicitudes de acceso a la información pública o de protección de datos personales, así como para la publicación y actualización de información pública fundamental, proactiva y focalizada. II. Realizar un análisis fundado y motivado para la reserva de información pública, en el que se observe lo previsto en el artículo 18 de la Ley, el cual deberá remitir para su revisión y consideración al Comité de Transparencia del sujeto obligado a través de la Unidad de Transparencia correspondiente. III. Realizar la búsqueda exhaustiva de la información pública, ante una inexistencia de información pública, y remitir al Comité de Transparencia correspondiente, a través de su Unidad de Transparencia, un informe sobre sus resultados. Dicho informe deberá detallar las circunstancias de modo, tiempo y lugar de la búsqueda, señalar el nombre del servidor público que tuvo bajo su resguardo la información en última instancia y, en su caso, la fundamentación y motivación que sustente la inexistencia de la información; IV. Certificar a través de su titular, las constancias y documentos que obren en sus archivos; V. Asistir a las capacitaciones y reuniones de trabajo a las que sean convocados por la Coordinación o su Unidad de Transparencia; VI. Realizar en tiempo y forma el llenado de los formatos de información que correspondan a su área, derivado del ejercicio de sus funciones, cargarlos y actualizarlos mensualmente en el sistema de la Plataforma Nacional de Transparencia correspondiente, así como remitir a su Unidad de Transparencia los formatos cargados y acuses electrónicos que emita la Plataforma Nacional de Transparencia; VII. Remitir a la Unidad de Transparencia que corresponda, los argumentos necesarios y manifestaciones respecto a los agravios expresados en los recursos de revisión, de transparencia y de protección de datos personales, o en las quejas relacionadas con el sistema de obligaciones de transparencia de la Plataforma Nacional de Transparencia; VIII. Proporcionar la información necesaria para dar cumplimiento a las resoluciones del Instituto, dentro del término requerido por la Unidad de Transparencia; IX. Adoptar las medidas de seguridad de carácter administrativo, técnico y físico que señala la Ley de Datos Personales, a efecto de garantizar la protección de los datos

	personales; X. Permitir el acceso a la Coordinación para la revisión de los procedimientos en materia de acceso a la información pública, obligaciones de transparencia y protección de datos personales, así como a la información pública que corresponda para tales efectos; y, XI. Designar los enlaces necesarios al interior de su estructura para el cumplimiento de las obligaciones establecidas en el presente Reglamento, quienes deberán permanecer en comunicación constante con el personal de su Unidad de Transparencia y su Comité.	
Datos personales incluidos en el Sistema/Inventario:		
Inventario de datos personales: Nivel de protección: Alto	Nombre, domicilio, CURP, RFC, sueldos, características físicas, correos electrónicos, número de teléfono particular, características del vehículo.	
Tipo de tratamiento:	Tratamiento no automatizado y automatizado	
Tiempo de resguardo de los datos personales:	De acuerdo a la normatividad vigente	
Transferencia de ficheros que puede ser objeto la información confidencial.		
Instancia	**Finalidad**	**Nivel de protección**
Coordinación General Estratégica de Seguridad	Entregar información referente expedientes de solicitudes de información o de acceso a datos personales, cuando sea requerida por un juzgado o por el ministerio público.	Alto

REGISTROS DE DATOS CONTENIDOS EN LA NÓMINA DE LOS SERVIDORES PÚBLICOS CON FUNCIONES OPERATIVAS Y/O ADMINISTRATIVAS DE LA COORDINACIÓN GENERAL ESTRATÉGICA DE SEGURIDAD.	
Datos de identificación:	
Fecha de Elaboración:	16 de agosto de 2021
Sujeto Obligado:	Coordinación General Estratégica de Seguridad

Unidad Administrativa Responsable:	Coordinación General Administrativa
Nombre y cargo del responsable	Mtra. Ingrid Guerrero Lobato, Coordinadora Administrativa del Coordinación General Estratégica de Seguridad
Contenido del Sistema:	
Finalidad de sistemas y los usos previstos.	Recabar los datos para integrar los expedientes de los servidores públicos que laboran en esta dependencia.
Las personas o grupos de personas sobre las cuales se obtienen los datos.	Servidores públicos adscritos a la Coordinación General Estratégica de Seguridad
Procedimiento de recolección	Se recaban documentos y se realizan entrevistas.
Tipo de soporte en donde se contienen los datos personales:	Documentos físicos y archivos electrónicos.
Medidas de seguridad:	Administrativas: se lleva bitácora de acceso Físicas: se cuenta con archivero bajo llave y oficina ajena a personas externas las cual también se encuentra bajo llave en la oficina del Director General de Gestión Pública. Técnicas: equipos con clave de acceso y archiveros cerrados con llave
Lugar y características del resguardo	Computadoras con clave y usuario, y archiveros en oficinas con llave.
Estructura básica del sistema y la descripción de los tipos de datos incluidos:	
Área:	Coordinación administrativa
Responsable y Administradores:	Mtra. Ingrid Guerrero Lobato, LTS. Yulissa Sarai Torres Romero
Cargo:	Coordinadora Administrativa del Coordinación General Estratégica de Seguridad, Coordinador Administrativo C
Domicilio:	Avenida Unión no. 292, Col. Deitz, Calle Herrera y Cairo no. 1034,Col. Villaseñor, Guadalajara, Jalisco, C.P. 44200.
Teléfono:	36687927 extensión 18168 36687971 extensión 18134
Correo electrónico:	transparencia.cges@jalisco.gob.mx
Administradores:	
Nombre:	Mtra. Ingrid Guerrero Lobato
Área:	Coordinación General Administrativa

Cargo:	Coordinadora Administrativa del Coordinación General Estratégica de Seguridad
Funciones y obligaciones:	I. Desempeñar las funciones de su competencia y comisiones que el Coordinador le delegue y encomiende, así como mantenerlo informado sobre el desarrollo de sus actividades; II. Participar en los convenios y contratos en que intervenga la Coordinación y que afecten su presupuesto, así como en los demás instrumentos jurídicos que impliquen actos de administración, y revisar los que celebren las dependencias agrupadas y entidades sectorizadas a la Coordinación, siempre y cuando dicha revisión sea solicitada por el titular de la Coordinación; III. Elaborar los proyectos de manuales y demás instrumentos administrativos que en general se requieran para el adecuado funcionamiento de la Coordinación; IV. Establecer, con la aprobación del Coordinador, las normas, sistemas y procedimientos para la administración de los recursos humanos, materiales y financieros de la Coordinación, en los términos de la normatividad aplicable; V. Auxiliar a las áreas administrativas de las dependencias agrupadas y entidades sectorizadas en materia de manuales de procedimientos en el ámbito de su competencia; 9 MARTES 4 DE AGOSTO DE 2020 / Número 35. Sección IIIACUERDO Al margen un sello que dice: Instituto de Transparencia, Información Pública y Protección de Datos Personales del Estado de Jalisco. 3 JUEVES 16 DE ENERO DE 2020 / Número 49. Sección II VI. Aplicar dentro de su ámbito de atribuciones, las políticas generales que regirán en la Coordinación y en las dependencias agrupadas y entidades sectorizadas a ésta, en cuanto a nombramientos, contratación, selección, remuneraciones, desarrollo y control del personal, así como sobre sanciones administrativas; VII. Conducir las relaciones laborales de la propia Coordinación, conforme a las disposiciones aplicables a los lineamientos que al efecto establezca el titular de la misma; VIII. Elaborar y someter a la consideración del Coordinador el anteproyecto de presupuesto anual de la Coordinación, así como autorizar las erogaciones, vigilar el ejercicio del presupuesto y llevar su contabilidad; IX. Proponer e impulsar proyectos para la simplificación administrativa de procesos, trámites y servicios en la Coordinación, así como en las dependencias agrupadas y entidades sectorizadas; X. Coordinar y coadyuvar en el funcionamiento de las áreas administrativas de las dependencias agrupadas y entidades sectorizadas; XI. Coordinar el seguimiento de los indicadores de los planes, proyectos y programas establecidos con la Secretaría de Planeación y Participación Ciudadana de aplicación en la Coordinación y en las dependencias agrupadas y entidades sectorizadas; XII. Impulsar la elaboración de diagnósticos de los procesos de las dependencias agrupadas y entidades sectorizadas para la mejora de la regulación en materia de seguridad y procuración de justicia conforme a la normatividad aplicable; XIII. Fomentar y establecer acciones para la administración adecuada de los recursos humanos, materiales y tecnológicos en la Coordinación y en las dependencias agrupadas y entidades sectorizadas; XIV. Coordinar la elaboración de los planes, programas y proyectos de la Coordinación y de las áreas administrativas de las dependencias agrupadas y entidades sectorizadas, con el fin de mejorar el ejercicio de sus funciones; XV. Coadyuvar en el ámbito de su especialización a las dependencias agrupadas y entidades sectorizadas; XVI. Proponer al Coordinador las medidas técnicas y administrativas que estime convenientes para la mejor organización y funcionamiento de la Coordinación y de las dependencias agrupadas y entidades sectorizadas, así como la eficiente ejecución de la modernización administrativa interna; XVII. Elaborar en coordinación con las dependencias agrupadas y entidades sectorizadas a la Coordinación los análisis de la

	detección de necesidades de capacitación y supervisar su cumplimiento en colaboración con el área competente; XVIII. Establecer instrumentos de evaluación de indicadores de gestión en cumplimiento a los planes, proyectos y programas de aplicación de la Coordinación y en las dependencias agrupadas y entidades sectorizadas; XIX. Establecer y coordinar el programa anual de adquisiciones de la Coordinación; XX. Realizar los trámites administrativos necesarios para la correcta operatividad de la Coordinación; XXI. Coordinar el efectivo aprovechamiento de los recursos federales en la Coordinación y en las dependencias agrupadas y entidades sectorizadas, y gestionar la obtención de recursos en las diferentes instancias de gobierno; y 10 ACUERDO Al margen un sello que dice: Instituto de Transparencia, Información Pública y Protección de Datos Personales del Estado de Jalisco. 3 MARTES 4 DE AGOSTO DE 2020 / Número 35. Sección III JUEVES 16 DE ENERO DE 2020 / Número 49. Sección IIACUERDO Al margen un sello que dice: Instituto de Transparencia, Información Pública y Protección de Datos Personales del Estado de Jalisco. 3 JUEVES 16 DE ENERO DE 2020 / Número 49. Sección II XXII. Las demás que establezcan otras disposiciones legales aplicables o que le confiera el
Nombre:	LTS.YulissaSarai Torres Romero
Área:	Coordinación General Administrativa de la Coordinación General Estratégica de Seguridad
Cargo	Coordinador Administrativo C
Funciones y obligaciones:	Coordinar las actividades relacionadas con la administración del personal como reclutamiento, selección y movimientos del personal, a fin de asegurar que el personal cuente con sus derechos como servidores públicos.
	Gestionar los trámites administrativos de bajas del personal para garantizar una adecuada separación del personal y que reciba el finiquito correspondiente.
	Organizar y llevar el control de la plantilla de personal autorizada, a fin de orientar al Coordinador Administrativo en la dotación del personal en tiempo y forma.
	Asistir al Coordinador Administrativo en los movimientos de la banca electrónica a fin de facilitar los trámites de pagos a proveedores.
	Elaborar oficios y documentos diversos que requiere la Coordinación Administrativa para el cumplimiento de sus actividades.
	Las demás que le confieran las disposiciones legales; así como aquellas que sean delegadas por sus superiores jerárquicos.
Datos personales incluidos en el Sistema/Inventario:	
Tipo de datos personales:	Huella digital, Numero de seguro social, Tipo de Sangre, Certificados, Trayectoria

Nivel de protección: Básico	Educativa, Cartilla Militar, Correo Electrónico, CURP, Domicilio, Edad, Estado Civil, Fecha de nacimiento, Firma, Fotografía, Idioma, Lugar de nacimiento, Nacionalidad, Nombre, Nombre de Familiares, dependientes y beneficiarios, RFC, Sexo, Teléfono celular, Teléfono particular, Referencias laborales, Referencias personales (Cartas de recomendación), Trabajo actual, Trabajos anteriores, cuentas bancarias, Ingresos y Egresos.	
Tipo de tratamiento:	Tratamiento automatizado y no automatizado. Archivos manuales y electrónicos.	
Tiempo de resguardo de los datos personales:	El tiempo que determina la ley o en su caso el área que corresponde	
Transferencia de ficheros que pueden ser objeto la información confidencial.		
Instancia	Finalidad	Nivel de protección
N/A	N/A	N/A

LIBRO DE GOBIERNO, PROPIAMENTE DE REGISTRO DE VISITANTES QUE INGRESAN A LA COORDINACIÓN GENERAL ESTRATÉGICA DE SEGURIDAD.	
Datos de identificación:	
Fecha de Elaboración:	16 de agosto de 2021
Sujeto Obligado:	Coordinación General Estratégica de Seguridad
Unidad Administrativa Responsable:	Coordinación General Administrativa de la Coordinación General Estratégica de Seguridad
Contenido del Sistema:	
Finalidad de sistemas y los usos previstos.	Se recaban los datos para llevar el control de ingresos y egresos a las oficinas de la Coordinación General Estratégica de Seguridad.
Las personas o grupos de personas sobre las cuales se obtienen los datos.	Personas físicas, y/o representantes de personas jurídicas y/o morales que visitan las instalaciones públicas de este Sujeto Obligado. Servidores públicos que no cuentan con gafete. Ciudadanos que acuden a las instalaciones.
Procedimiento de recolección	Físico en listas de ingreso.
Tipo de soporte en donde se contienen los datos personales:	Los datos personales se encuentran en soporte físico (libros de gobierno).
Medidas de seguridad:	Administrativas: Se encuentra bajo el resguardo de la Seguridad. Físicas: Se guardará en un archivero con llave
Lugar y características del resguardo	Resguardados en oficina con llave que solo personal autorizado tiene acceso, y escritorios con llave.
Estructura básica del sistema y la descripción de los tipos de datos incluidos:	
Área:	Coordinación General Administrativa de la Coordinación General Estratégica de Seguridad
Responsable y Administradores:	Mtra. Ingrid Guerrero Lobato, LTS.YulissaSarai Torres Romero
Cargo:	Coordinación General Administrativa de la Coordinación General Estratégica de Seguridad, Coordinador Administrativo C
Domicilio:	Avenida Unión no. 292, Col. Americana
Teléfono:	36687927 extensión 18168 36687971 extensión 18134
Correo electrónico:	transparencia.cges@jalisco.gob.mx

Área:	Dirección General de Gestión Pública	
Administradores:		
Coordinación General Administrativa	Mtra. Ingrid Guerrero Lobato	
Coordinador Administrativo C	LTS.Yulissa Sarai Torres Romero	
Datos personales incluidos en el Sistema/Inventario:		
Inventario de datos personales:	Nombre y Firma.	
Tipo de tratamiento:	Manual	
Nivel de seguridad:	Básico	
Tiempo de resguardo de los datos personales:	El tiempo que determina la ley o en su caso el área que corresponde	
Transferencia de ficheros que pueden ser objeto la información confidencial.		
Instancia	Finalidad	Nivel de protección
No se realizan transferencias	No se realizan transferencias	No se realizan transferencias

REGISTRO DE ASISTENCIA	
Datos de identificación:	
Fecha de Elaboración:	16 de agosto de 2021
Sujeto Obligado:	Coordinación General Estratégica de Seguridad
Unidad Administrativa Responsable:	Coordinación General Administrativa
Nombre y cargo del responsable	Mtra. Ingrid Guerrero Lobato, Coordinadora Administrativa de la Coordinación General Estratégica de Seguridad
Contenido del Sistema:	
Finalidad de sistemas y los usos previstos.	Recabar los datos biométricos para el control de las asistencias del personal adscrito a la Coordinación General Estratégica de Seguridad
Las personas o grupos de personas sobre las cuales se obtienen los datos.	Servidores públicos adscritos a la Coordinación General Estratégica de Seguridad
Procedimiento de recolección	Lectura de datos biométricos del personal mediante el sistema de registro de asistencia
Tipo de soporte en donde se contienen los datos personales:	Electrónico
Medidas de seguridad:	Administrativas: una sola persona de la Coordinación Administrativa es la autorizada mediante usuario y contraseña para el manejo adecuado de la información Físicas: elmanejo de la información es de manera electrónica Técnicas: se exporta la información a un formato electrónico
Lugar y características del resguardo	Se ubica en la recepción principal al ingreso del inmueble, bajo resguardo de la Coordinación Administrativa

Estructura básica del sistema y la descripción de los tipos de datos incluidos:	
Área:	Coordinación administrativa
Responsable y Administradores:	Mtra. Ingrid Guerrero Lobato, Lic. Gabriel Enrique Elías Flores, Lic. Roxana Barraza Valenzuela
Cargo:	Coordinadora Administrativa del Coordinación General Estratégica de Seguridad,Especialista Administrativo, Coordinador Especializado K
Domicilio:	Avenida Unión no. 292, Col. Deitz, Calle Herrera y Cairo no. 1034,Col. Villaseñor, Guadalajara, Jalisco, C.P. 44200.
Teléfono:	36687900 extensión 18168 36687971 extensión 18134
Correo electrónico:	transparencia.cges@jalisco.gob.mx
Administradores:	
Nombre:	Mtra. Ingrid Guerrero Lobato
Área:	Coordinación General Administrativa
Cargo:	Coordinadora Administrativa del Coordinación General Estratégica de Seguridad
Funciones y obligaciones:	I. Desempeñar las funciones de su competencia y comisiones que el Coordinador le delegue y encomiende, así como mantenerlo informado sobre el desarrollo de sus actividades; II. Participar en los convenios y contratos en que intervenga la Coordinación y que afecten su presupuesto, así como en los demás instrumentos jurídicos que impliquen actos de administración, y revisar los que celebren las dependencias agrupadas y entidades sectorizadas a la Coordinación, siempre y cuando dicha revisión sea solicitada por el titular de la Coordinación; III. Elaborar los proyectos de manuales y demás instrumentos administrativos que en general se requieran para el adecuado funcionamiento de la Coordinación; IV. Establecer, con la aprobación del Coordinador, las normas, sistemas y procedimientos para la administración de los recursos humanos, materiales y financieros de la Coordinación, en los términos de la normatividad aplicable; V. Auxiliar a las áreas administrativas de las dependencias agrupadas y entidades sectorizadas en materia de manuales de procedimientos en el ámbito de su competencia; 9 MARTES 4 DE AGOSTO DE 2020 / Número 35. Sección IIIACUERDO Al margen un sello que dice: Instituto de Transparencia, Información Pública y Protección de Datos Personales del Estado de Jalisco. 3 JUEVES 16 DE ENERO DE 2020 / Número 49. Sección II VI. Aplicar dentro de su ámbito de atribuciones, las políticas generales que regirán en la Coordinación y en las dependencias agrupadas y entidades sectorizadas a ésta, en cuanto a nombramientos, contratación, selección, remuneraciones, desarrollo y control del personal, así como sobre sanciones administrativas; VII. Conducir las relaciones laborales de la propia Coordinación, conforme a las disposiciones aplicables a los lineamientos que al efecto establezca el titular de la misma; VIII. Elaborar y someter a la consideración del Coordinador el anteproyecto de presupuesto anual de la Coordinación, así como autorizar las erogaciones, vigilar el ejercicio del presupuesto y llevar su contabilidad; IX. Proponer e impulsar proyectos para la simplificación administrativa de procesos, trámites y servicios en la Coordinación, así como en las dependencias agrupadas y entidades sectorizadas; X. Coordinar y coadyuvar en el funcionamiento de las áreas administrativas de las dependencias agrupadas y entidades sectorizadas; XI. Coordinar el seguimiento de los indicadores de los planes, proyectos y programas establecidos con la Secretaría de Planeación y Participación Ciudadana de aplicación en la Coordinación y en las dependencias agrupadas y entidades sectorizadas; XII. Impulsar la elaboración de

	diagnósticos de los procesos de las dependencias agrupadas y entidades sectorizadas para la mejora de la regulación en materia de seguridad y procuración de justicia conforme a la normatividad aplicable; XIII. Fomentar y establecer acciones para la administración adecuada de los recursos humanos, materiales y tecnológicos en la Coordinación y en las dependencias agrupadas y entidades sectorizadas; XIV. Coordinar la elaboración de los planes, programas y proyectos de la Coordinación y de las áreas administrativas de las dependencias agrupadas y entidades sectorizadas, con el fin de mejorar el ejercicio de sus funciones; XV. Coadyuvar en el ámbito de su especialización a las dependencias agrupadas y entidades sectorizadas; XVI. Proponer al Coordinador las medidas técnicas y administrativas que estime convenientes para la mejor organización y funcionamiento de la Coordinación y de las dependencias agrupadas y entidades sectorizadas, así como la eficiente ejecución de la modernización administrativa interna; XVII. Elaborar en coordinación con las dependencias agrupadas y entidades sectorizadas a la Coordinación los análisis de la detección de necesidades de capacitación y supervisar su cumplimiento en colaboración con el área competente; XVIII. Establecer instrumentos de evaluación de indicadores de gestión en cumplimiento a los planes, proyectos y programas de aplicación de la Coordinación y en las dependencias agrupadas y entidades sectorizadas; XIX. Establecer y coordinar el programa anual de adquisiciones de la Coordinación; XX. Realizar los trámites administrativos necesarios para la correcta operatividad de la Coordinación; XXI. Coordinar el efectivo aprovechamiento de los recursos federales en la Coordinación y en las dependencias agrupadas y entidades sectorizadas, y gestionar la obtención de recursos en las diferentes instancias de gobierno; y 10 ACUERDO Al margen un sello que dice: Instituto de Transparencia, Información Pública y Protección de Datos Personales del Estado de Jalisco. 3 MARTES 4 DE AGOSTO DE 2020 / Número 35. Sección III JUEVES 16 DE ENERO DE 2020 / Número 49. Sección IIACUERDO Al margen un sello que dice: Instituto de Transparencia, Información Pública y Protección de Datos Personales del Estado de Jalisco. 3 JUEVES 16 DE ENERO DE 2020 / Número 49. Sección II XXII. Las demás que establezcan otras disposiciones legales aplicables o que le confiera el
Nombre:	Lic. Fabian Ching Chávez
Área:	Coordinación Administrativa de la Coordinación General Estratégica de Seguridad
Cargo	Coordinador Especializado A
Funciones y obligaciones:	Coordinar las actividades relacionadas con la administración del personal como reclutamiento, selección y movimientos del personal, a fin de asegurar que el personal cuente con sus derechos como servidores públicos.
	Gestionar los trámites administrativos de bajas del personal para garantizar una adecuada separación del personal y que reciba el finiquito correspondiente.
	Organizar y llevar el control de la plantilla de personal autorizada, a fin de orientar al Coordinador Administrativo en la dotación del personal en tiempo y forma.
	Asistir al Coordinador Administrativo en los movimientos de la banca electrónica a fin de facilitar los trámites de pagos a proveedores.
	Elaborar oficios y documentos diversos que requiere la Coordinación Administrativa para el cumplimiento de sus actividades.
	Las demás que le confieran las disposiciones legales; así como aquellas que sean delegadas por sus superiores jerárquicos.
Datos personales incluidos en el Sistema/Inventario:	

Tipo de datos personales:	Huella digital, nombre y número de identificación de los servidores públicos	
Nivel de protección: Básico		
Tipo de tratamiento:	Tratamiento automatizado	
Tiempo de resguardo de los datos personales:	El tiempo que determina la ley o en su caso el área que corresponde	
Transferencia de ficheros que pueden ser objeto la información confidencial.		
Instancia	Finalidad	Nivel de protección
No se realizan transferencias a instituciones externas	N/A	N/A

IV. RESPONSABILIDADES Y OBLIGACIONES DE LAS PERSONAS QUE TRATAN DATOS PERSONALES

Para garantizar la aplicación correcta de los sistemas de tratamiento de datos personales, es necesario establecer los deberes de los servidores públicos de la Coordinación General Estratégica de Seguridad que participan en el tratamiento de los datos personales derivado de sus atribuciones.

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

1) Tener a la vista el Aviso de Privacidad.

2) Dar a conocer el aviso de privacidad al titular de los datos personales previo a la obtención de sus datos.

3) En caso de dudas o quejas de los titulares de los datos personales sobre el tratamiento de sus datos, orientar al ciudadano para que acuda a la Unidad de Transparencia.

4) Al obtener los datos personales cerciorarse de que la información esté completa, actualizada, sea veraz, y comprensible.

5) Comunicar discrepancias de los datos personales recabados a su jefe inmediato o al administrador de los datos personales, ello cuando se percate.

6) Conocer y seguir las medidas de seguridad que le sean aplicables para el cuidado de los datos personales, durante el periodo en el que posea los datos personales.

7) Recabar los datos personales **para la finalidad** para la cual estos fueron recabados según el trámite o el sistema de tratamiento que corresponda.

8) Conocer, aplicar y sujetarse al Aviso de Privacidad y al Documento de Seguridad de la Coordinación General Estratégica de Seguridad en el tratamiento de datos personales.

9) Guardar estricta **confidencialidad** de los datos personales que conozca en el ejercicio de sus funciones.

10) Sujetarse a lo establecido en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco.

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

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

1) Conocer, aplicar y sujetarse al Aviso de Privacidad y al Documento de Seguridad de la Coordinación General Estratégica de Seguridad, en el tratamiento de datos personales.

2) Aplicar las medidas de seguridad correspondientes a los datos personales tratados y/o el sistema de protección en el que participa.

3) Tratar los datos personales siguiendo los principios establecidos en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco.

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

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

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

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

8) Sujetarse a lo establecido en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco.

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

1) Conocer, aplicar y sujetarse al Aviso de Privacidad y al Documento de Seguridad de la Coordinación General Estratégica de Seguridad, en el tratamiento de datos personales.

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

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

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

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

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

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

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

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

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

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

12) Acudir a la Unidad de Transparencia en caso de asesoría sobre el tratamiento de datos personales.

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

14) Dar aviso al Comité de Transparencia, a través de la Unidad de Transparencia, sobre las actas circunstanciadas de hechos levantadas por el incumplimiento del documento de seguridad y sobre el seguimiento de las mismas.

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

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

1) Conocer, aplicar y sujetarse al Aviso de Privacidad y al Documento de Seguridad de la Coordinación General Estratégica de Seguridad, en el tratamiento de datos personales.

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

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

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

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

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

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

8) Monitorear la implementación de las medidas de seguridad.

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

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

11) Presentar propuestas de mejora o modificación del documento de seguridad a través de la Unidad de Transparencia.

12) Emitir reportes en relación al tratamiento de los datos personales y la aplicación de medidas de seguridad, según sea requerido por el Comité de Transparencia a través de la Unidad de Transparencia.

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

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

Son obligaciones de la Unidad de Transparencia en relación al tratamiento de datos personales, además de las previstas en el artículo 88 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco:

1) Difundir al interior de sujeto Obligado el aviso de privacidad y el documento de seguridad.

2) Revisión física anual a sobre el tratamiento de datos personales y la implementación de medidas de seguridad.

3) Proponer al Comité de Transparencia actualizaciones o modificaciones al documento de seguridad.

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

Son obligaciones del Comité de Transparencia en relación al tratamiento de datos personales, además de las previstas en el artículo 87 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco:

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

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

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

V. DE LAS MEDIDAS DE SEGURIDAD

Para la seguridad de los datos personales, la Coordinación General Estratégica de Seguridad (CGES) establece medidas de seguridad físicas, administrativas y físicas.

Las medidas de seguridad administrativas se traducen en políticas y procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, la identificación, clasificación y borrado seguro de la información, así como la sensibilización y capacitación del personal, en materia de protección de datos personales.

Las medidas de seguridad físicas son el conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento.

Las medidas técnicas son el conjunto de acciones y mecanismos que se valen de la tecnología relacionada con hardware y software para proteger el entorno digital de los datos personales y recursos involucrados en su tratamiento.

La CGES tiene implementadas medidas de seguridad mismas que son reflejadas de forma particular en cada uno de los sistemas de tratamiento. Además la CGES cuenta con medidas de seguridad que son

implementadas desde la Unidad de Transparencia, que es la que gestiona la implementación de lo establecido en el Documento de Seguridad. A continuación se describen estas medidas:

MEDIDAS DE SEGURIDAD ESTABLECIDAS EN LOS SISTEMAS DE TRATAMIENTO	
Administrativas	Llave controlada por una sola persona. Acceso de personas autorizadas a los espacios exclusivos donde se encuentran los expedientes.
Físicas	Expediente dentro de espacios exclusivos Expedientes dentro de muebles de archivo Archivos protegidos bajo llave en una oficina con puerta de acceso a la que solo personal del área de Archivo tiene acceso.
Técnicas	Base de datos en equipos de cómputo que cuentan con contraseña de acceso Ingreso a los Sistemas por medio de Usuarios y Contraseñas Se realizan respaldos de la información semanalmente

MEDIDAS DE SEGURIDAD ESTABLECIDAS POR LA UNIDAD DE TRANSPARENCIA	
Administrativas	Uso de las bitácoras: • Control de acceso • Transferencias • Vulneraciones Revisiones semestrales a las áreas para comprobar el grado de apego a lo

	establecido en el documento de seguridad. Carta compromiso de confidencialidad del manejo de datos personales, firmada por el personal de nuevo ingreso. Constancia y acuse de recibo para transferencia de documentos físicos. Constancia para transferencia de documentos electrónicos. Se capacita al personal que trabajan con datos personales por lo menos una vez al año, se cuentan con 3 capacitaciones al año en diferentes temas, se va capacitando al personal específico de los temas impartidos
Físicas	Eliminación y entrega de los medios de almacenamiento: Los medios deberán eliminarse de modo seguro cuando no se les necesite más, usando procedimientos formales Los expedientes físicos y electrónicos que contienen datos personales no se tienen al alcance de cualquier persona. Prevenir el acceso no autorizado a la Coordinación General Estratégica de Seguridad, sus instalaciones físicas, áreas críticas, recursos e información. Se cuentan con procedimientos y medidas de seguridad recomendadas y aplicables por Protección Civil al interior de las instalaciones. Proteger los Recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir de la Coordinación General Estratégica de Seguridad. Se cuentan con mecanismos y acciones que permiten identificar los equipos móviles y portátiles: mobiliario, documentos y materiales mediante controles de entrada y salida, tales como: control en el ingreso y egreso de aparatos, equipos, mobiliarios, documentos y materiales mediante la autorización por los titulares de las áreas. En la mayoría de las áreas, el acceso (al área donde se recibe a los ciudadanos y se recaban datos personales) se tiene restringido, una vez que el dato se encuentra en posesión del servidor público, es decir si fue recabado frente a un escritorio, área abierta o pasillo, los ciudadanos no podrán pasar detrás de estos, ya que al terminar de recabar datos estos se colocan fuera del alcance de los ciudadanos. La oficina cuenta con puertas que cierra el área al momento de terminar labores. Las llaves que se tienen de la oficina se encuentran en manos de servidores

	públicos, autorizados por el área general. Cada carpeta de trámites o archivo, al terminar el proceso de cada uno, son resguardados en un archivo de cada área. El aviso de privacidad se encuentra a la vista y alcance de los ciudadanos, es decir en el espacio físico donde se recaban los datos personales.
Técnicas	El acceso a las bases de datos es exclusivo para aquellos cuyas áreas o unidades responsables de la información han autorizado. Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware. Las áreas son responsables de validar el perfil del usuario que se apegue a lo necesario, para cumplir con las funciones de los sistemas de información, las áreas son responsables de los procesos respectivos. Respaldos semanales por parte del área de informática.

Controles y medidas de seguridad para las Transferencias

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

- Toda solicitud de transferencia de datos personales deberá ser formalizada mediante oficio.
- Solo podrán ser transferidos los datos personales para dar seguimiento y conclusión al trámite o sistema de tratamiento bajo la finalidad que éstos prevean.
- El área que entrega los datos personales deberá cerciorarse de transferir la totalidad de los datos que resulten necesarios para el seguimiento o la conclusión del trámite o sistema de tratamiento correspondiente. Limitándose a la entrega de datos adicionales que no resulten necesarios.
- El área que entrega los datos personales deberá cerciorarse de que los datos que transfiere sean completos y veraces.
- El área que reciba los datos personales deberá conservar los mismos sujetándose a las finalidades y lineamientos del aviso de privacidad de este sujeto obligado y adoptando las medidas de seguridad previstas en este documento.
- El área que reciba los datos personales deberá encargarse de la supresión de los datos que reciba cuando esta corresponda.
- La entrega de datos personales se deberá realizar mediante oficio dirigido al responsable del resguardo o al administrador de los datos personales. Los documentos que contengan los datos

personales deberán de entregarse en un sobre cerrado y con una constancia que acredite cuando se le entrega y que se entrega. La constancia deberá estar firmada por el responsable de la entrega.

- En el caso de que algún área receptora no permita la recepción en sobre cerrado de los documentos que contienen datos personales, entonces el área emisora deberá plasmar en el oficio de entrega que se hace una transferencia de datos personales y deberá anexar además la constancia.

- El área responsable del resguardo, que realizará la transferencia, contará con una bitácora en donde realizará los registros por cada una de las transferencias realizadas, lo anterior para tener el control histórico de las transferencias. (Anexo 1. Bitácora de transferencias de datos personales).

- En el caso de que el oficio de respuesta contenga datos personales, éste deberá de ir en sobre cerrado. El formato de Acuse de Recibo de Ejercicio de Derechos ARCO fungirá como el acuse de recibo. (Anexo 2)

Transferencias a Externos:

- El tercero que reciba los datos personales deberá sujetarse a las finalidades y lineamientos del aviso de privacidad de este sujeto obligado y deberá adoptar las medidas de seguridad previstas en este documento.

- Toda solicitud de transferencia de datos personales deberá ser formalizada mediante oficio.

- La entrega de datos personales se deberá realizar mediante oficio dirigido al funcionario autorizado de recibir los datos personales. Los documentos que contengan los datos personales deberán de entregarse en un sobre cerrado y con una constancia que acredite cuando se le entrega y que se entrega. La constancia deberá estar firmada por el responsable de la entrega.

- El área responsable del resguardo, que realizará la transferencia, contará con una bitácora en donde realizará los registros por cada una de las transferencias realizadas, lo anterior para tener el control histórico de las transferencias. (Anexo 1. Bitácora de transferencias de datos personales)

- En el caso de que el oficio de respuesta contenga datos personales, éste deberá de ir en sobre cerrado. El formato de Acuse de Recibo de Ejercicio de Derechos ARCO fungirá como el acuse de recibo. (Anexo 2).

- En el caso que alguna autoridad no acepte sobre cerrado, deberá de manifestarse la entrega de los datos personales mediante el oficio de respuesta.

VI. BITÁCORAS DE TRANSFERENCIAS, ACCESO Y VULNERACIONES A LA SEGURIDAD DE LOS DATOS PERSONALES

Bitácora de Transferencias de Datos Personales (Anexo 3)

Esta bitácora es utilizada para el registro de la transferencia de los datos personales, ya sea entre áreas internas o externasy contiene la siguiente información:

- Fecha
- Tipo de entrega
- Medio de entrega
- Área, dependencia o autoridad a la que se transfieren los datos personales
- Datos personales que se transfieren
- Nombre de la persona autorizada para la entrega de los datos personales
- Nombre de la persona que recibe los datos personales

Bitácora de Acceso a los Datos Personales(Anexo 4)

La bitácora de acceso a los datos personales se utilizasólo en los casos de que se trate de expedientes físicos y contienen 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
- Hora de Devolución

2. Las bitácoras se pueden encontrar en soporte físico o electrónico.

3. Son resguardadas por los coordinadores de cada área o por los responsables de los procesos que involucran datos personales, en el lugar que para tal efecto designen.

Vulneraciones a la Seguridad de los Datos Personales (Anexo 5)

La bitácora de vulneraciones se utiliza cuando el área tiene alguna vulneración en la seguridad de los datos personales, ya sea por una pérdida o destrucción no autorizada, el robo, extravío o copia no autorizada; el uso, acceso o tratamiento no autorizado; o el daño, la alteración o modificación no autorizada.La bitácora de vulneraciones contiene 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.

Una vez detectada la vulneración se debe de notificar al titular de los datos personales y al titular de la Unidad de Transparencia, quién a su vez deberá notificar al Instituto lo siguiente:

I. La naturaleza del incidente;

II. Los datos personales comprometidos;

III. Las recomendaciones y medidas que el titular puede adoptar para proteger sus intereses;

IV. Las acciones correctivas realizadas de forma inmediata; y

V. Los medios donde puede obtener mayor información al respecto

VII. ANÁLISIS DE RIESGOS

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

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

- Alteración de la información.
- Intromisión de personas ajenas a la red y a las bases de datos electrónicas de este sujeto obligado. (Hackers)

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

ORIGEN DE LA AMENAZA	CAUSA	POSIBLES CONSECUENCIAS
Acceso de personas no autorizadas a los sistemas o plataformas oficiales del sujeto obligado.	Adquirir información o datos personales.	Acceso no autorizado. Divulgación de datos personales. Robo de información. Modificaciones no autorizadas. Robo de información.
Acceso de personas no autorizadas como criminales o traficantes de datos a los sistemas o plataformas oficiales del sujeto obligado.	Adquirir datos personales para utilizarlos con fines de explotación, chantaje, extorsión o cualquier uso criminal.	Extorsiones. Ataques a personas. Robo de información. Vulneración a la seguridad física y mental de los ciudadanos. Robo de información.
Personal del sujeto obligado con poco conocimiento sobre el tratamiento de datos personales.	Obtener información para beneficio personal. Curiosidad. Error involuntario. Por fines económicos.	Ataque a otros servidores públicos. Robo de información. Pérdida de datos personales. Uso indebido de datos personales. Uso ilícito de datos personales. Robo de información. Extorsión. Modificaciones no autorizadas. Robo de información.
Daño físico.	Agua. Fuego. Accidentes. Corrosión.	Daño o pérdida de los datos personales.

ORIGEN DE LA AMENAZA	CAUSA	POSIBLES CONSECUENCIAS
Eventos naturales.	Desastres climatológicos. Fenómenos meteorológicos. Sismos. Cualquier eventualidad por causa natural.	Daño o pérdida de los datos personales.
Fallas técnicas.	Pérdida de electricidad. Falla o pérdida de internet. Falla en sistemas, correos electrónicos o plataformas oficiales.	Daño o pérdida de los datos personales. Divulgación y transferencia de datos personales. Modificaciones no autorizadas.
Decadencias técnicas.	Mantenimiento insuficiente. Falla en equipos. Poca o absoluta renovación de equipos de telecomunicaciones o cómputo. Cambios de voltaje.	Pérdida, destrucción y daño.
Susceptibilidad en redes o sistemas autorizados.	Falta de contraseñas altamente efectivas. Falta de mecanismos para identificar o autenticación de usuarios. Falta de actualización de antivirus.	Pérdida, destrucción y daño. Divulgación y transferencia de datos personales. Modificaciones no autorizadas. Robo de información.
Organización.	Procesos carentes de formalidad para administración, acceso, uso y proceso de archivo.	Pérdida, destrucción y daño. Divulgación y transferencia de datos personales. Modificaciones no autorizadas. Robo de información. Robo de información.
Espacio donde se archiven.	Carencia de espacio. Espacio con poca seguridad. Espacio no adecuado. Falta de llaves o medidas de seguridad para accesos.	Daño o pérdida de los datos personales. Divulgación y transferencia de datos personales. Modificaciones no autorizadas. Robo de información.

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

VIII. ANÁLISIS DE BRECHA

TEMA	ESTADO ACTUAL	PARÁMETRO
Seguridad institucional	Transferencias en sobre cerrado con constancia de información confidencial anexa. Transferencias en electrónico con la constancia de información confidencial adjunta.	Que todas las áreas de este sujeto obligado estén utilizando esta medida de control.
Activos del responsable	Cada una de las áreas de este sujeto obligado, cuenta con un padrón del personal que accede a los datos personales.	Otorgar la responsabilidad a cada uno de los servidores públicos que gestionan datos personales, para que apliquen las medidas de seguridad establecidas en sus respectivos sistemas de tratamiento.

Seguridad en recursos humanos	Se cuenta con una carta compromiso de protección de datos personales para el personal de nuevo ingreso	La carta compromiso de datos personales se mantiene, incrementando el personal del sujeto obligado que ya cuente con su firma en ella.
Recolección de datos personales	Quien recaba los datos personales, es un servidor público del área, asignado especialmente para recabar datos en general	Quien recaba los datos personales, es un servidor público del área, asignado especialmente para recabar datos en general, únicamente los necesarios derivados del ejercicio de sus atribuciones y facultades.
Red	Política de uso de los servicios de red: Los usuarios sólo deben contar con acceso a los servicios para los que han sido autorizados.	Bloquear o dar de baja puertos y servicios innecesarios en equipos de cómputo.
Contraseñas	Uso de contraseñas: Se deberá exigir a los usuarios que trabajen sobre todo datos sensibles y de un nivel alto de protección que sigan buenas prácticas de seguridad en la selección y uso de las contraseñas.	Contraseña de mínimo 10 caracteres
Equipos	Los usuarios deberán asegurar que los equipos atendidos cuenten con protección adecuada.	Considerar bloqueo automático del equipo a los 5 minutos con solicitud de contraseña para desbloquear.
Resguardo	Los archivos que contienen datos personales se encuentran en archiveros o muebles con cajones.	Todos los archiveros, muebles, lockers que resguardan archivos de datos personales, deberán contar con llave.Las llaves de los archiveros con las que se cuentan se encuentran en posesión de servidores públicos encargados del área
Capacitación	Se han realizado durante el año 2019, tres capacitaciones referentes a datos personales	Se realiza un mínimo de tres capacitaciones anuales en el tema de datos personales, con asistencia mínima de 100 personas.
Procedimientos	Se cuenta con las directrices y controles para la protección de los	Socialización al personal de las directrices y controles, plasmados

	datos personales,registrados en el documento de seguridad.	en el manual de procedimientos del sujeto obligado.

IX. GESTIÓN DE VULNERACIONES

El proceso es el siguiente:

FLUJOGRAMA	DETALLE NARRATIVO
 Inicio	Se presenta contingencia en el área
El área se percata de lo sucedido	El área detecta que existe una vulneración en las bases de datos que contienen datos personales. La vulneración puede ser ocasionada por el daño, pérdida, alteración, destrucción o uso, acceso o tratamiento no autorizado de los datos personales.
El área registra evento en bitácora de vulneraciones	El encargado de la bitácora de vulneración del área registra los siguientes datos: • Fecha en que ocurrió la vulneración. • Motivo de la vulneración. • Datos personales comprometidos. • Acciones correctivas implementadas • Medidas a adoptar por el titular de los datos para proteges sus intereses. • Nombre y cargo de quién lo reporta. • Firma de quién reporta.
El área notifica a la Unidad de Transparencia sobre la eventualidad	Después del registro, se deberá informar por escrito,anexando la bitácora de vulneraciones al titular de la Unidad de Transparencia sobre las vulneraciones de seguridad ocurridas, las que afecten o impacten de forma significativa los derechos patrimoniales o morales del titular; lo anterior en un plazo máximo de setenta y dos horas.
La UT registra en formato el evento	Registra el anexo 6 y envía al ITEI los pormenores del evento de vulneración.

La UT notifica mediante oficio al ITEI anexando el formato 6	Envía al ITEI por oficio la notificación del evento de vulneración, anexando el anexo 6.
El responsable del área planea e implementa acciones preventivas y correctivas	Al ocurrir una vulneración de seguridad, el servidor público titular del área responsable y/o el responsable del sistema deberá analizar la causa por lo que ocurrió dicha vulneración, e implementar acciones preventivas y correctivas para adecuar medidas de seguridad que prevengan esta eventualidad, para evitar que la vulneración se repita. A su vez, en caso de detectar que la falla fue ocasionada por el incumplimiento de un servidor público a su cargo deberá levantar acta circunstanciada de hechos correspondiente y seguir el procedimiento administrativo correspondiente ante la Dirección General Jurídica.
Fin	El ITEI es notificado

X. CONTROLES PARA LA IDENTIFICACIÓN Y AUTENTIFICACIÓN DE USUARIOS:

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

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

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

El estándar para la creación de las cuentas es:

Usuario: nombre de usuario
Contraseña: Frase de confirmación de identidad que se encuentra encriptada para mayor seguridad.

Estos accesos son dados, por parte de la Dirección de Tecnologías de la Información y Comunicaciones, área donde se lleva el control de usuarios y contraseñas otorgadas mediante una carta responsiva personalizada la cual va firmada por el interesado y la persona que autoriza.

Todas las computadoras precisan de un nombre de usuario y contraseña para ingresar.

2. Los empleados de la Coordinación General Estratégica de Seguridad deben portar en todo momento su identificación institucional que cuenta con la siguiente información:

Al frente:

- Nombre
- Cargo
- Vigencia
- Número de Empleado

Al reverso:

- Firma del interesado
- Firma del Titular de la Institución
- Domicilio de la Institución

3. A los ciudadanos se les solicita identificación oficial con fotografía, cuando ingresa a las instalaciones o cuando es necesario que acrediten su identidad ente el sujeto obligado.

XI. DEL PLAN DE TRABAJO

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

La finalidad de este plan es plasmar de manera enunciativa, más no limitativa, las actividades que la Coordinación General Estratégica de Seguridadrealizará para la aplicación del presente documento de seguridad

Cronograma
Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados del Estado de Jalisco y sus Municipios

Plan de Trabajo para la actualización, aplicación de los Documentos de Seguridad y Avisos de Privacidad de las Unidades de Transparencia Gobierno del Estado de Jalisco.

Este plan de trabajo tiene como finalidad integrar y dar asesoría a las Unidades de Transparencia para dar seguimientoa la actualizacióndel Aviso de Privacidad y del Documento de Seguridad, para cumplir con las obligaciones en materia de protección y tratamiento de los datos personales recabados por cada sujeto obligado.

Plan de Trabajo.

Aviso de Privacidad.

1. El aviso de privacidad es un documento físico y electrónico o en cualquier formato generado por el responsable, mismo que tiene que ser puesto a disposición del titular ya sea de forma física, electrónica o por cualquier medio masivo de comunicación con el objeto de informarle los propósitos principales del tratamiento al que serán sometidos sus datos personales.(Art 3 III)

2. El titular deberá tener conocimiento del aviso de privacidad previo al tratamiento a que serán sometidos sus datos personales. El aviso de privacidad Integral deberá ser difundido por los medios electrónicos y físicos con que se cuente, tales como medios impresos, sonoros, digitales, visuales o cualquier otra tecnología; con una redacción y estructura clara y sencilla, para cumplir con el propósito de informar, deben estar publicados obligatoriamente en: (Art 3 XXIV).

    - Portal de transparencia en articulo 8 Información Fundamental fracción IX como información proactiva, también en la parte superior derecha del portal (debajo de lo datos de la unidad de transparencia).
    - Impresos y colocados en los escritorio, lugar de trabajo y ventanillas de donde se recaban los datos personales.
    - Todos aquellos micro sitios que recaben datos personales por contener encuestas o trámites.
    - En casos específicos como el aviso de privacidad de video cámaras deben publicarse en los edificios, específicamente en lugares estratégicos que estén a la vista de los ciudadanos.
    - Cuando se recaben datos personales vía telefónica deberá ponerse a disposición de los ciudadanos el aviso de privacidad corto e informar donde puede consultar el aviso de privacidad integral.

3. Es importante considerar que los datos personales recabados por el responsable deberán ser tratados únicamente para finalidades establecidas en el aviso de privacidad, en caso de existir cambios en las atribuciones conferidas en la ley se modifican las mismas en el aviso de privacidad (Art 26); el responsable podrá tratar los datos personales para distintas finalidades a las previstas en el aviso de privacidad siempre que medie el consentimiento expreso del titular (Art 11.3), para recabar el consentimiento deberá tener una ¨carta consentimiento¨(Art 14.2).

4. Cabe destacar que cuando los datos personales hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas en el aviso de privacidad y que motivaron su tratamiento conforme a las disposiciones aplicables, deberán ser suprimidos de conformidad con su propio mecanismo (Art 17 .1 y .2), previo bloqueo en su caso y una vez que concluya el plazo de conservación de los mismos (Art 5 fracción V y XXXIV).

5. EL aviso de privacidad se pondrá a disposición del titular en tres modalidades corto, simplificado e integral, descripción breve de las modalidades del aviso de privacidad (Art 21-25):

   - El aviso de privacidad corto se usará cuando el espacio utilizado para la obtención de los datos sea mínimo y limitado, de igual forma, los datos solicitados por el responsable deberán ser los básicos, el mismo aviso deberá contener:
     I. La identidad y domicilio del responsable;
     II. Las finalidades del tratamiento; y
     III. Los mecanismos que el responsable ofrece para que el titular conozca el aviso de privacidad integral.

   - El aviso simplificado deberá contener la siguiente información:
     I. La denominación del responsable;
     II. Las finalidades del tratamiento para las cuales se obtienen los datos personales, distinguiendo aquellas que requieran el consentimiento del titular;
     III. Cuando se realicen transferencias de datos personales que requieran consentimiento, se deberá informar:
     a) Las autoridades, poderes, entidades, órganos y organismos gubernamentales de los tres órdenes de gobierno y las personas físicas o morales a las que se transfieren los datos personales;
     b) Las finalidades de estas transferencias.
     IV. Los mecanismos y medios disponibles para que el titular, en su caso, pueda manifestar su negativa para el tratamiento de datos personales para finalidades y transferencias que requieren el consentimiento del titular; y
     V. El sitio donde se podrá consultar el aviso de privacidad integral.

     Esta modalidad de aviso de privacidad será puesto a disposición en los siguientes momentos:
     I. Cuando los datos personales se obtienen de manera directa del titular previo a la obtención de los mismos;
     II. Cuando los datos personales se obtienen de manera indirecta del titular previo al uso o aprovechamiento de éstos.
     Las reglas anteriores no eximen al responsable de proporcionar al titular el aviso de privacidad integral en un momento posterior, conforme a las disposiciones aplicables de esta Ley.

   - Información, aviso de privacidad integral, deberá contener al menos, la siguiente información:

I. El domicilio del responsable;
II. Los datos personales que serán sometidos a tratamiento, identificando aquellos que son sensibles;
III. El fundamento legal que faculta al responsable para llevar a cabo el tratamiento;
IV. Las finalidades del tratamiento para las cuales se obtienen los datos personales, distinguiendo aquellas que requieren el consentimiento del titular;
V. La información sobre el uso de mecanismos en medios remotos o locales de comunicación electrónica, óptica u otra tecnología, que permita recabar datos personales de manera automática y simultánea al tiempo que el titular hace contacto con los mismos, en su caso;
VI. Los mecanismos, medios y procedimientos disponibles para ejercer los derechos ARCO;
VII. El domicilio de la Unidad de Transparencia;
VIII. Los medios a través de los cuales el responsable comunicará a los titulares los cambios al aviso de privacidad.

En toda transferencia de datos personales, el responsable deberá comunicar al receptor de los datos personales el aviso de privacidad, comprometiéndose a garantizar su confidencialidad y únicamente los utilizará para los fines que fueron transferidos atendiendo a lo convenido en el aviso de privacidad que le será comunicado por el responsable transferente, el receptor adquiere carácter de responsable (Art 72).

Ejemplos:

- Al momento de celebrar un contrato y en el mismo se faculte la transferencia de datos, este deberá contener cláusula donde se adhiere al aviso de privacidad de quien transfiere los datos.
- Cuan por trámite diverso que conlleve la transferencia de datos personales utilizados en esfera externa al servicio público.

Documento de Seguridad.

1. El **Documento de Seguridad** es un instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee, el cual a actualmente se encuentra realizado, no obstante se tiene la obligación de actualizarlo. (Art 37)

2. Una vez integrado el Documento de Seguridad el responsable **deberá revisar** el documento de seguridad de manera periódica, así como **actualizar su contenido** cuando ocurran los siguientes eventos:

I. Se produzcan modificaciones sustanciales al tratamiento de datos personales que deriven en un cambio en el nivel de riesgo;
II. Como resultado de un proceso de mejora continua, derivado del monitoreo y revisión del sistema de gestión;
III. Como resultado de un proceso de mejora para mitigar el impacto de una vulneración a la seguridad ocurrida; y
IV. Se implementen acciones correctivas y preventivas ante una vulneración de Seguridad ocurrida.

3. El responsable deberá establecer controles o mecanismos que tengan por objeto que todas aquellas personas que intervengan en cualquier fase del tratamiento de los datos personales guarden confidencialidad respecto de éstos, obligación que subsistirá aún después de finalizar sus relaciones con el mismo.(Art 44)

Atribuciones del comité relativas al aviso de privacidad y documento de seguridad.(Art 87)

1. **Aprobar, supervisar** y evaluar las políticas, programas, acciones y demás actividades que correspondan para el cumplimiento de la presente Ley y demás disposiciones aplicables.
2. Derivado de lo anterior se considera que se deberá **generar un programa de actualización** anual del **aviso de privacidad y documento de seguridad**, por Unidad de Transparencia.
3. Derivado de la **aplicación del programa de actualizaciones** se deberá sesionar para aprobar el **programa de trabajo** para las actualizaciones al aviso de privacidad y documento de seguridad.
4. Deberá sesionar para aprobar las actualizaciones del aviso de privacidad y documento de seguridad.

Cronograma del plan de trabajo para actualizar el Documento de Seguridad						
Actividad	**Duración (días)**	**Fecha inicio**	**Fecha fin**	**Resultados Esperados**	**Entregables**	**Observaciones**
Análisis del documento de seguridad vigente.	5	Última semana de abril 2021	Última semana de abril 2021	Determinar situación actual documento de seguridad.	Diagnóstico para actualización del documento de seguridad.	Análisis interno
Envío, recepción y revisión de sistemas de tratamiento a las unidades administrativa para actualización	40	Primera semana de mayo 2021	Última semana de junio 2021	Análisis y modificación de información por las unidades administrativas	Formatos actualizados	Análisis interno y en coordinación con las áreas
Integración del documento de seguridad con la información actualizada	10	Primera semana de julio 2021	Segunda semana de julio 2021	Información actualizada enviada por las áreas integrada	Documento integrado	Análisis interno
Sesión del comité para la aprobación de actualizaciones del aviso de privacidad.	2	Segunda semana de agosto 2021	Segunda semana de agosto 2021	Aprobación de la actualización del Documento de Seguridad.	Acta de la sesión correspondiente	Gestión de firmas
Socialización del documento de seguridad	2	Cuarta semana de agosto 2021	Cuarta semana de agosto 2021	Publicar y difundir el documento de seguridad actualizado.	Publicación en la información fundamental y aviso mediante oficio a las unidades administrativa del sujeto obligado	Conocimiento del documento por parte del personal

Cronograma del plan de trabajo para actualizar el Aviso de Privacidad						
Actividad	**Duración (días)**	**Fecha inicio**	**Fecha fin**	**Resultados Esperados**	**Entregables**	**Observaciones**
Análisis del aviso de privacidad actual.	5	Segunda semana de febrero 2021	Segunda semana de febrero 2021	Determinar situación actual del Aviso de Privacidad	Aviso de privacidad analizado.	Análisis interno
Propuesta del Aviso de Privacidad y visto bueno Coordinación General de Transparencia	10	Tercera semana de febrero 2021	Cuarta semana de febrero 2021	Borrador de aviso de privacidad autorizado	Documento con visto bueno	Revisión por la Coordinación General de Transparencia
Actualización del documento de seguridad	45	Última semana de abril 2021	Última semana de junio 2021	Información actualizada enviada por las áreas integrada	Documento integrado	El documento de seguridad sirve como insumo del Aviso de Privacidad
Adaptación del documento de seguridad según inventario de los sistemas de tratamiento	5	Primera semana de julio 2021	Primera semana de julio 2021	Aviso de privacidad alineado a los sistemas de tratamiento	Avisos de Privacidad en sus tres versiones, actualizados	Análisis interno
Revisión por el enlace	5	Segunda semana de julio 2021	Segunda semana de julio 2021	Revisión del aviso de privacidad	Autorización del aviso de privacidad	Gestión de firmas
Sesión del comité para la aprobación de actualizaciones del aviso de privacidad.	2	Segunda semana de agosto 2021	Segunda semana de agosto 2021	Aprobación de la actualización del Documento de Seguridad.	Acta de la sesión correspondiente	Gestión de firmas
Socialización del documento de seguridad	2	Cuarta semana de agosto 2021	Cuarta semana de agosto 2021	Publicar y difundir el documento de seguridad actualizado.	Publicación en la información fundamental y aviso mediante oficio a las unidades	Conocimiento del documento por parte del personal

					administrativa del sujeto obligado	

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

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

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

Mecanismos de monitoreo. Objetivo del monitoreo.	Objetivo del monitoreo.
Revisión en campo en las unidades administrativas para la revisión de las medidas de seguridad	Verificar la aplicación, actualización e impacto de las medidas de seguridad aplicadas, descritas en el documento de seguridad.

XIII. EL PROGRAMA GENERAL DE CAPACITACIÓN

Se manejarán dos capacitaciones anuales dirigidas a los enlaces de datos personales de las áreas.

Las fechas exactas se les notificarán a los Enlaces de Transparencia con al menos una semana de anticipación a las fechas estimadas con la intención de que éstos las difundan con los interesados en asistir a las capacitaciones.

El programa de capacitación es el siguiente:

Tema	Asistentes	Objetivo	Facilitadores	Año
Uso Test Data 2.0	Personal de la Unidad de Transparencia y enlaces de las áreas administrativas	Desarrollar el conocimiento en el procedimiento y las generalidades de la creación de versiones públicas	Coordinación General de Transparencia, en conjunto con la Dirección de Transparencia y Buenas Prácticas del Ayuntamiento de	Agosto 2021

			Guadalajara	
Difusión del Documento de Seguridad y reforzamiento de las medidas de seguridad en las unidades administrativas de la Secretaría de Seguridad	Enlaces y sub enlaces de las unidades administrativas de la Secretaría de Seguridad	Que el personal conozca el documento de seguridad y y cuente con habilidades técnicas para proteger los datos personales, ya sea con las medidas físicas, técnicas y administrativas así como con los controles necesarios en el caso de transferencias.	Unidad de Transparencia de la Coordinación General Estratégica de Seguridad	2021

XIV. ANEXOS

ANEXO 1. CONSTANCIA DE PROTECCIÓN DE INFORMACIÓN CONFIDENCIAL

Unidad de Transparencia de la Coordinación
General Estratégica de Seguridad

Coordinación de Seguridad
GOBIERNO DE JALISCO

CONSTANCIA DE PROTECCIÓN DE INFORMACIÓN CONFIDENCIAL

Se remite la solicitud de información, misma que contiene Datos Personales de acuerdo a lo establecido con el artículo 3, fracción IX de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios.

En ese tenor y en concordancia con el artículo 75 punto 1, fracción II de la Ley antes citada, se transfiere información confidencial, **como lo son datos personales del solicitante de información, consistente en [Especificar el tipo de datos que se transfieren, pertenecientes a la persona o personas identificada(s) o identificable(s)].** lo anterior a efecto de que pueda dar respuesta al solicitante. Dando cumplimiento a lo establecido en nuestro aviso de confidencialidad que dispone que los terceros receptores de los datos personales pueden ser; los sujetos obligados a los que se dirijan las solicitudes de información pública que sean de su competencia con la finalidad de darle seguimiento; así como al órgano de control interno de este sujeto obligado, en caso de que se dé vista por el posible incumplimiento a la Ley que rige la materia. Lo anterior de conformidad a lo establecido en el capítulo II, Título Segundo, artículos 87 y 88 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios, así como en el numeral 25 de la citada Ley, so pena de las responsabilidades y Sanciones previstas en los cuerpos normativos en comento.

Se adjunta la presente, de conformidad con el artículo 71 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios, y los Lineamientos Cuadragésimo Segundo y Cuadragésimo Tercero de los Lineamientos Generales para la Protección de la Información Confidencial y Reservada que deberán de observar los Sujetos Obligados previstos en la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios.

[Nombre]
[Cargo]

ANEXO 2. ACUSE DE SOLICITUD DE EJERCICIO DE DERECHOS ARCO

Unidad de Transparencia de la Coordinación
General Estratégica de Seguridad y Secretaría de Seguridad

ACUSE DE SOLICITUD DE EJERCICIO DE DERECHOS ARCO

Se remite la solicitud de ejercicio de derechos ARCO, misma que contiene Datos Personales de acuerdo a lo establecido con el artículo 3, fracción IX de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios.

EXPEDIENTE.- **LPDPJ/CGES/0000/2019**
NÚMERO DE OFICIO.-
DIRIGIDO.-
FECHA DE DERIVACIÓN DE SOLICITUD A TRAVÉS DE MEDIOS ELECTRÓNICOS:

FECHA Y HORARIO DE RECEPCION DE DOCUMENTO._____

FIRMA DE RECIBIDO_____

En ese tenor y en concordancia con el artículo 75 punto 1, fracción II de la Ley antes citada, se transfiere información confidencial, **como lo son datos personales del solicitante de información, consistente en los datos que derivan del reporte de servicio de emergencia,** lo anterior a efecto de que pueda dar respuesta al solicitante. Dando cumplimiento a lo establecido en nuestro aviso de confidencialidad que dispone que los terceros receptores de los datos personales pueden ser; los sujetos obligados a los que se dirijan las solicitudes de información pública que sean de su competencia con la finalidad de darle seguimiento.

Lo anterior de conformidad a lo establecido en el capítulo II, Título Segundo, artículos 87 y 88 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios, así como en los numerales 25 y 26 de la citada Ley, so pena de las responsabilidades y Sanciones previstas en los cuerpos normativos en comento.
JSPM/AM

ANEXO 3. BITÁCORA DE TRANSFERENCIAS DE DATOS PERSONALES

BITÁCORA DE TRANSFERENCIAS DE DATOS PERSONALES

COORDINACIÓN GENERAL ESTRATÉGICA DE SEGURIDAD

Fecha	Tipo de entrega (Electrónica, física, por red, otros)	Medio de entrega	Área, dependencia o autoridad a la que se le tranfieren los datos personales	Datos personales transferidos	Nombre de la persona autorizada para la entrega de los datos personales	Firma de la persona autorizada para la entrega de los datos personales	Nombre de la persona autorizada para recibir los datos personales

ANEXO 4. BITÁCORA DE ACCESO A LOS DATOS PERSONALES

BITÁCORA DE ACCESO DE LOS DATOS PERSONALES

COORDINACIÓN GENERAL ESTRATÉGICA DE SEGURIDAD

Nombre y cargo de quien accede	Identificación del expediente	Fojas del expediente	Propósito del acceso	Fecha del acceso	Hora del acceso	Fecha de devolución	Hora de devolución

ANEXO 5. BITÁCORA DE VULNERACIÓN DE LOS DATOS PERSONALES

BITÁCORA DE VULNERACIÓN DE LOS DATOS PERSONALES

COORDINACIÓN GENERAL ESTRATÉGICA DE SEGURIDAD

Fecha en que ocurrió la vulneración	Motivo de la vulneración	Datos personales comprometidos	Acciones correctivas implementadas	Medidas a adoptar por el titular de los datos para proteger sus intereses	Nombre y cargo de quién reporta	Firma de quién reporta

ANEXO 6. VULNERACIONES A LOS SISTEMAS DE INFORMACIÓN Y BASES DE DATOS

Coordinación de Seguridad
GOBIERNO DE JALISCO

Secretaría de Seguridad

VULNERACIONES A LOS SISTEMAS DE INFORMACIÓN Y BASES DE DATOS

Descripción del evento de vulneración	
Causas de la vulneración	
Nombre del responsable de la investigación	
Cargo	
Área	
Número de investigación	
La información vulnerada se encuentra en el documento de seguridad	Si ☐ No ☐
Fecha en que se creó el sistema de información o la base de datos vulnerada	
Fundamento legal para la obtención de los datos personales	
Resguardo de los soportes	
Usuarios	
Medidas de seguridad físicas, técnicas y administrativas	
Administrador del sistema de información o base de datos vulnerada	
Medidas correctivas implementadas	