Coordinación de Seguridad
GOBIERNO DE JALISCO

2020

DOCUMENTO DE SEGURIDAD

COORDINACIÓN GENERAL ESTRATÉGICA DE SEGURIDAD

Coordinación de Seguridad
GOBIERNO DE JALISCO

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, y asimismo mediante el acuerdo respectivo se concentra la Unidad de Transparencia de la Coordinación General Estratégica de Seguridad y la Secretaría de Seguridad, así como se crea el Comité de Transparencia de la Coordinación General Estratégica de Seguridad y Secretaría 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.

Es importante aclarar que la Secretaría de Seguridad se encuentra sectorizada a la Coordinación General Estratégica de seguridad y ambos forman un solo sujeto obligado llamado coordinación General Estratégica de Seguridad. Sin embargo se decidió realizar un documento por los dos entes públicos con el fin de que cada uno registre sus propias particularidades. Este documento en particular, responde a cubrir las necesidades y obligaciones que tiene 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:	
Sujeto Obligado:	
Unidad Administrativa Responsable:	
Nombre y Cargo del Responsable:	
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 registrar el trámite que se le otorga a cada una de ellas.
Las personas o grupos de personas sobre las cuales se obtienen los datos.	
Procedimiento de recolección	
Tipo de soporte en donde se contienen los datos personales:	
Medidas de Seguridad:	
Resguardo de los Soportes Físicos y/o electrónicos:	
Estructura básica del sistema y la descripción de los tipos de datos incluidos:	
Área:	Unidad de Transparencia
Responsable y Administradores:	Titular de la Unidad de Transparencia, Mtro. Javier Sosa Pérez Maldonado
Cargo:	Titular 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:	Responsable: Mtro. Javier Sosa Pérez Maldonado Administradores: Adriana Alejandra López Robles y José Luis Huerta Vázquez.
Área:	Unidad de Transparencia
Cargo:	Titular de la Unidad de Transparencia

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:	Nombre, domicilio, CURP, RFC, sueldos, características físicas, correos electrónicos, número de teléfono particular, características del vehículo.	
Nivel de protección: Alto		
Tipo de tratamiento:	Tratamiento no automatizado y automatizado	
Transferencia de ficheros que puede ser objeto la información confidencial.		
Instancia	**Finalidad**	**Nivel de protección**
	Entregar solicitudes de información o de acceso a datos personales, a sujetos obligados que tengan una competencia total, parcial o concurrente.	
	Entregar información referente a solicitudes de información, cuando sea requerida por un juzgado o por el ministerio público.	
	Entregar información referente a solicitudes de información, cuando sea requerida por un juzgado o por el ministerio público.	

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:	
Sujeto Obligado:	
Unidad Administrativa Responsable:	
Nombre y cargo del responsable	
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.	
Procedimiento de recolección	
Tipo de soporte en donde se contienen los datos personales:	
Medidas de seguridad:	
Lugar y características del resguardo	
Estructura básica del sistema y la descripción de los tipos de datos incluidos:	
Área:	

Responsable y Administradores:	
Cargo:	
Domicilio:	
Teléfono:	
Correo electrónico:	
Administradores:	
Nombre:	
Área:	
Cargo:	
Funciones y obligaciones:	**Reglamento Interno de la Coordinación Estratégica de Seguridad** Artículo 13 Corresponde a la Dirección General de Gestión Pública el ejercicio de las siguientes atribuciones: I. Acordar con el Coordinador los asuntos de su competencia y de las unidades administrativas a su cargo. III. Establecer, con la aprobación del Coordinador, las normas, sistemas y procedimientos para la administración de los recursos humanos, materiales y financieros de la Coordinación y de las dependencias y entidades sectorizadas, en los términos de la normatividad aplicable; IV. Establecer, dentro de su ámbito de atribuciones, las políticas generales que regirán en la Coordinación y en las dependencias y entidades sectorizadas a ésta, en cuanto a nombramientos, contratación, selección, remuneraciones, desarrollo, control e incentivos del personal, así como sobre sanciones administrativas; V. Desarrollar los sistemas de premios, estímulos y recompensas, así como los reconocimientos que determinen las Condiciones Generales de Trabajo y las disposiciones jurídicas aplicables; VI. Conducir las relaciones laborales de la Coordinación, conforme a las disposiciones aplicables a los lineamientos que al efecto establezca el titular de la misma, así como supervisar y establecer lineamientos generales para las dependencias y entidades sectorizadas a la Coordinación; VII. Planear y conducir la política de desarrollo del personal, definir los puestos tipo y establecer los perfiles y requerimientos de los mismos, así como las formas de identificación del personal, y establecer políticas o lineamientos generales de aplicación en las dependencias y entidades sectorizadas a la Coordinación; XII. Fomentar la administración adecuada de los recursos humanos, materiales y tecnológicos en la Coordinación y en las dependencias y entidades sectorizadas a ésta; XIII. Establecer acciones para la adecuada administración de los recursos económicos, materiales y humanos en la Coordinación y en las dependencias y entidades sectorizadas a ésta;

	XVI. Acordar la liquidación y pago de cualquier remuneración al personal de la Coordinación; XXII. Elaborar y supervisar, en su ámbito de atribuciones, políticas de contratación del personal para el funcionamiento de la Coordinación y de las dependencias y entidades sectorizadas a la Coordinación; XXVI. Fungir como órgano de control disciplinario para la instauración del procedimiento administrativo de responsabilidad en contra de servidores públicos de la Coordinación, de conformidad a lo establecido en la Ley para los Servidores Públicos del Estado de Jalisco y sus Municipios, asesorando en su caso a las distintas áreas organizacionales en los asuntos relacionados con este tema;
Nombre:	
Área:	
Cargo	
Funciones y obligaciones:	Reglamento Interno de la Secretaría de Seguridad Artículo 15. La Dirección Administrativa tendrá a su cargo las siguientes facultades: V. Evaluar el cumplimiento de las políticas y obligaciones administrativas y financieras correspondientes en las dependencias y entidades sectorizadas a la Coordinación; VII. Desarrollar las políticas y lineamientos en materia administrativa de obligatorias para la Coordinación y las dependencias y entidades sectorizadas a ésta; VIII. Auxiliar al Director General de Gestión Pública en el cumplimiento de las obligaciones financieras y administrativas, en el marco de sus atribuciones;
Nombre:	Lic. Víctor Francisco Cervantes Franco.
Área:	Dirección Administrativa de la Coordinación General Estratégica de Seguridad.
Cargo:	Director Administrativo de la Coordinación General Estratégica de Seguridad.
Funciones y obligaciones:	Reglamento Interno de la Coordinación General Estratégica de Seguridad del Poder Ejecutivo del Estado de Jalisco Artículo 15. La Dirección Administrativa tendrá a su cargo las siguientes facultades: I. Elaborar el anteproyecto de presupuesto de egresos de la Coordinación y supervisar el de las de las dependencias y entidades sectorizadas a ésta; II. Supervisar de manera periódica a las dependencias y entidades sectorizadas a la coordinación en las áreas de competencias de la Dirección General de Gestión Pública; III. Elaborar, en coordinación con las áreas administrativas de la Coordinación General, los anteproyectos de presupuesto asignado para la presentación, revisión, aprobación y aplicación;

	IV. Asesorar en materia financiera y administrativa respecto al diseño de planes, programas y proyectos a las dependencias y entidades sectorizadas a la Coordinación; VI. Proponer e impulsar proyectos para la modernización y simplificación de procesos, trámites y servicios en la Coordinación en las dependencias y entidades sectorizadas a ésta; IX. Coordinar e implementar proyectos que impulsen la cultura de calidad en el servicio de la Coordinación en las dependencias y entidades sectorizadas a ésta; X. Establecer los lineamientos para la elaboración de los manuales administrativos y de procesos de la Coordinación y de las dependencias y entidades sectorizadas a ésta, de conformidad con la normatividad aplicable; XI. Brindar asesoría a las dependencias y entidades sectorizadas a la Coordinación en el ámbito de su competencia; XII. 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 y entidades sectorizadas a ésta. XIII. Coordinar el efectivo aprovechamiento de los recursos federales en la Coordinación y en las dependencias y entidades sectorizadas a ésta. XIV. Gestionar la obtención de recursos en las diferentes instancias de gobierno, y a nivel internacional; XV. Coadyuvar con el área competente en la generación de los planes de capacitación y el eficiente uso de los recursos; y XVI. Las demás que establezcan otras disposiciones legales aplicables o que le confiera el Coordinador y/o el Director General de Gestión Pública.
Administradores:	Director General de Gestión Pública, Director General Administrativo de la Secretaría de Seguridad y Director General Administrativo de la Coordinación General Estratégica de Seguridad
Datos personales incluidos en el Sistema/Inventario:	
Inventario de datos personales: Nivel de protección: Básico	
Tipo de tratamiento: Tiempo de resguardo de los datos personales:	

Transferencia de ficheros que pueden ser objeto la información confidencial.		
Instancia	Finalidad	Nivel de protección

N/A	N/A	N/A

SISTEMA DE VIDEO VIGILANCIA ESCUDO URBANO	
Datos de identificación:	
Fecha de Elaboración:	
Sujeto Obligado:	
Unidad Administrativa Responsable:	
Nombre y cargo del responsable	
Contenido del Sistema:	
Finalidad de sistemas y los usos previstos.	Coordinación, Comando, Control, Video, Vigilancia para la prevención y detección oportuna ante situaciones de riesgos y eventos dentro del Estado de Jalisco
Las personas o grupos de personas sobre las cuales se obtienen los datos.	
Procedimiento de recolección	
Tipo de soporte en donde se contienen los datos personales:	
Medidas de seguridad:	
Lugar y características del resguardo	
Estructura básica del sistema y la descripción de los tipos de datos incluidos:	
Área:	
Responsable y Administradores:	
Cargo:	
Domicilio:	
Teléfono:	
Correo electrónico:	
Administradores:	
Nombre:	
Área:	
Cargo:	
Funciones y obligaciones:	**Ley Orgánica del Organismo Público Descentralizado Denominado Centro de Coordinación, Comando, Control, Comunicaciones y Cómputo Del Estado De Jalisco. Artículo:** **Artículo 20.** El personal administrativo y operativo que labore o sea comisionado al "Escudo Urbano C5" deberá: I. Observar las restricciones referentes a la reserva, control, análisis, utilización y uso de la información obtenida de los equipos y sistemas tecnológicos que señala la Ley ;

	II. Remitir la información a las autoridades administrativas, ministeriales o judiciales que así lo requieran, y en su caso, con apego al procedimiento de cadena de custodia previsto en los artículos 227 y 228 del Código Nacional de Procedimientos Penales; III. Autentificar por escrito la información que se entregue a las autoridades competentes en las remisiones y puestas a disposición que se realicen, precisando su origen y las circunstancias en que se allegó de ésta; IV. Implementar el procedimiento y cumplir con los requisitos establecidos en el capítulo correspondiente de la Ley, para la valoración de los medios de prueba que se obtengan y de conformidad con los artículos 251 y 252 del Código Nacional de Procedimientos Penales; V. Cumplir con las demás atribuciones que en materia de medios probatorios se prevé para las instituciones de seguridad pública en la Ley y artículos 251 y 252 del Código Nacional de Procedimientos Penales; y VI. El personal que labore en otras instalaciones al del "Escudo Urbano C5" deberá proporcionar aquella información captada mediante el uso de equipos y sistemas tecnológicos de video vigilancia, que le sea requerida por el Director General. **Artículo 26.** Al frente de la Dirección Operativa habrá un titular, a quien le corresponde el ejercicio de las siguientes funciones: I. Coordinar de forma permanente en los C2 Municipales y en el área de video vigilancia del "Escudo Urbano C5", cohesión y eficiencia en el comando, control y la dirección de las operaciones entre dependencias para la respuesta oportuna ante un incidente o un escenario de emergencia mayor; II. Ejecutar los planes, programas, así como garantizar el cumplimiento de las políticas y procedimientos para desempeño óptimo de la operación continuamente; III. Coordinar adecuadamente los procedimientos operativos con las diferentes instituciones para la atención eficiente de emergencias que se presenten en su área diariamente; y Las demás que le confieran las disposiciones legales aplicables y el Director General.
Datos personales incluidos en el Sistema/Inventario:	
Inventario de datos personales:	
Nivel de protección:	
Tipo de tratamiento:	
Tiempo de resguardo de los datos personales:	

Transferencia de ficheros que puede ser objeto la información confidencial.		
Instancia	**Finalidad**	**Nivel de protección**

	Coadyuvar con las autoridades en ejercicio de sus funciones en los procesos de tipo: Jurídico y administrativo derivadas de la normativa en materia de Seguridad Pública.	
	Tratamiento y transferencia de la información con discrecionalidad y respeto requeridos en el ejercicio de sus funciones para procesos de tipo jurídico y administrativo así como de investigación, bajo la norma en materia de Seguridad Pública.	

SEGURIDAD PÚBLICA INTEGRADOS AL CENTRO INTEGRAL DE COMUNICACIONES 911	
Datos de identificación:	
Fecha de Elaboración:	
Sujeto Obligado:	
Unidad Administrativa Responsable:	
Nombre y cargo del responsable	
Contenido del Sistema:	
Finalidad de sistemas y los usos previstos.	Optimizar las comunicaciones y la coordinación interinstitucional en situaciones de emergencia, entre los cuerpos de seguridad pública, de atención médica, y de protección civil, a efecto de que éstas cumplan con sus fines institucionales en beneficio del interés social.
Las personas o grupos de personas sobre las cuales se obtienen los datos.	
Procedimiento de recolección	
Tipo de soporte en donde se contienen los datos personales:	
Medidas de seguridad:	
Lugar y características del resguardo	
Estructura básica del sistema y la descripción de los tipos de datos incluidos:	
Área:	
Responsable y Administradores:	
Cargo:	
Domicilio:	
Teléfono:	
Correo electrónico:	
Administradores:	
Nombre:	
Área:	
Cargo:	
Funciones y obligaciones:	**Ley Orgánica del Organismo Público Descentralizado Denominado Centro de Coordinación, Comando, Control, Comunicaciones y Cómputo Del Estado De Jalisco.** **Artículo 6.** El “Escudo Urbano C5” tendrá las atribuciones siguientes:

	VI. Establecer comunicación directa y de coordinación con autoridades del ámbito federal, estatal o municipal, así como con instituciones y organismos privados, para la integración de bases de datos que resulten útiles para el cumplimiento sus atribuciones; X. Administrar y operar los servicios de Atención de Llamadas a Emergencia 911, Denuncia Anónima 089 y Locatel, mediante la recepción, registro y canalización de las solicitudes de auxilio, apoyo o denuncia que realice la ciudadanía, a las dependencias, órganos desconcentrados y entidades de la administración pública del Estado de Jalisco, así como a las instancias del ámbito federal, estatal o municipal, competentes para su atención; XI. Administrar y operar la línea telefónica única de asistencia a la población del Estado de Jalisco, a través del Servicio Público de Localización Telefónica, así como mediante el uso de nuevas tecnologías; XII. Planear y ejecutar acciones de difusión para el uso adecuado de los servicios de Atención de Llamadas a Emergencia 911, Denuncia Anónima 089 y de Localización Telefónica, así como de las herramientas tecnológicas e infraestructura de que dispone, con arreglo a la normatividad aplicable; XVII. Aprovechar la información captada a través de la sala de video monitoreo, de los Servicios de Atención de Llamadas a Emergencia 911 y Denuncia Anónima 089, del Servicio Público de Localización Telefónica, de las bases de datos que integra, así como de los sistemas o equipos de comunicación de que disponga, para el diseño de estrategias, implementación de mejoras, elaboración de estadísticas, generación de inteligencia y demás acciones que sean necesarias para el cumplimiento de sus atribuciones.
Datos personales incluidos en el Sistema/Inventario:	
Inventario de datos personales:	
Nivel de protección: Alto	
Tipo de tratamiento:	
Tiempo de resguardo de los datos personales:	

Transferencia de ficheros que puede ser objeto la información confidencial.		
Instancia	**Finalidad**	**Nivel de protección**
	Cumplimiento de obligaciones legales derivadas de la Normatividad en Materia de Seguridad Pública, requerida en el ejercicio de sus funciones.	
	Cumplimiento de obligaciones legales derivadas de la Normatividad en Materia de Seguridad Pública	

	Cumplimiento de obligaciones legales derivadas de la Normatividad en Materia de Seguridad Pública	

SISTEMA DE REGISTRO DE LLAMADAS A LA DIRECCIÓN GENERAL DEL CENTRO INTEGRAL DE COMUNICACIONES 911	
Datos de identificación:	
Fecha de Elaboración:	
Sujeto Obligado:	
Unidad Administrativa Responsable:	
Nombre y cargo del responsable	
Contenido del Sistema:	
Finalidad de sistemas y los usos previstos.	Registro y Control de las llamadas recibidas en el número telefónico único para atención de emergencias, denuncia anónima 089 y Locatel, para el despacho de servicios médicos, policiales y de protección civil, apoyados en un sistema integrado por personal capacitado, tecnología de cómputo y radiocomunicaciones.
Las personas o grupos de personas sobre las cuales se obtienen los datos.	
Procedimiento de recolección	
Tipo de soporte en donde se contienen los datos personales:	
Medidas de seguridad:	
Lugar y características del resguardo	
Estructura básica del sistema y la descripción de los tipos de datos incluidos:	
Área:	
Responsable y Administradores:	
Cargo:	
Domicilio:	
Teléfono:	
Correo electrónico:	
Administradores:	
Nombre:	
Área:	
Cargo:	
Funciones y obligaciones:	**Ley Orgánica del Organismo Público Descentralizado Denominado Centro de Coordinación, Comando, Control, Comunicaciones y Cómputo Del Estado De Jalisco.** **Artículo 6.** El “Escudo Urbano C5” tendrá las atribuciones siguientes:

	X. Administrar y operar los servicios de Atención de Llamadas a Emergencia 911, Denuncia Anónima 089 y Locatel, mediante la recepción, registro y canalización de las solicitudes de auxilio, apoyo o denuncia que realice la ciudadanía, a las dependencias, órganos desconcentrados y entidades de la administración pública del Estado de Jalisco, así como a las instancias del ámbito federal, estatal o municipal, competentes para su atención; XII. Planear y ejecutar acciones de difusión para el uso adecuado de los servicios de Atención de Llamadas a Emergencia 911, Denuncia Anónima 089 y de Localización Telefónica, así como de las herramientas tecnológicas e infraestructura de que dispone, con arreglo a la normatividad aplicable; XVII. Aprovechar la información captada a través de la sala de video monitoreo, de los Servicios de Atención de Llamadas a Emergencia 911 y Denuncia Anónima 089, del Servicio Público de Localización Telefónica, de las bases de datos que integra, así como de los sistemas o equipos de comunicación de que disponga, para el diseño de estrategias, implementación de mejoras, elaboración de estadísticas, generación de inteligencia y demás acciones que sean necesarias para el cumplimiento de sus atribuciones; **Artículo 25. Al frente de esta Dirección de Atención a Emergencias habrá un titular, a quien le corresponde el ejercicio de las siguientes funciones:** I. Dirigir y supervisar la operación de la Central de Llamadas 911/089, para la atención eficiente de emergencias y protección ciudadana, asegurando la calidad del servicio, así como la integración y coordinación operativa de las diferentes áreas y dependencias que intervienen en el "Escudo Urbano C5". III. Mejorar y supervisar la atención de llamadas de emergencia y atender los requerimientos de información; IV. Coordinar la operación del servicio de la Atención de Denuncia Anónima 089, así como la correcta recepción, registro y canalización de las denuncias anónimas que realiza la población vía telefónica u otro medio; V. Coordinar la operación del servicio telefónico de localización de personas
Datos personales incluidos en el Sistema/Inventario:	
Inventario de datos personales:	
Nivel de protección: Alto	
Tipo de tratamiento:	
Tiempo de resguardo de los datos personales:	

Transferencia de ficheros que puede ser objeto la información confidencial.		
Instancia	**Finalidad**	**Nivel de protección**
	Cumplimiento de obligaciones legales derivadas de la Normatividad en Materia de Seguridad Pública, requerida en el ejercicio de sus funciones.	
	Cumplimiento de obligaciones legales derivadas de la Normatividad en Materia de Seguridad Pública	

LIBRO DE GOBIERNO, PROPIAMENTE DE REGISTRO DE VISITANTES QUE INGRESAN A LA COORDINACIÓN GENERAL ESTRATÉGICA DE SEGURIDAD.	
Datos de identificación:	
Fecha de Elaboración:	
Sujeto Obligado:	
Unidad Administrativa Responsable:	
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 y Secretaría de Seguridad.
Las personas o grupos de personas sobre las cuales se obtienen los datos.	
Procedimiento de recolección	
Tipo de soporte en donde se contienen los datos personales:	
Medidas de seguridad:	
Lugar y características del resguardo	
Estructura básica del sistema y la descripción de los tipos de datos incluidos:	
Área:	
Responsable y Administradores:	
Cargo:	
Domicilio:	
Teléfono:	
Correo electrónico:	
Área:	
Administradores:	
Nombre:	
Área:	
Cargo:	
Funciones y obligaciones:	**Reglamento Interno de la Coordinación Estratégica de Seguridad** Artículo 13 Corresponde a la Dirección General de Gestión Pública el ejercicio de las siguientes atribuciones: I. Acordar con el Coordinador los asuntos de su competencia y de las unidades administrativas a su cargo. III. Establecer, con la aprobación del Coordinador, las normas, sistemas y procedimientos para la administración de los recursos humanos, materiales y financieros de la Coordinación y de las dependencias y entidades sectorizadas, en los términos de la normatividad aplicable; IV. Establecer, dentro de su ámbito de atribuciones, las políticas generales que regirán en la Coordinación y en las dependencias y entidades sectorizadas a ésta, en

	cuanto a nombramientos, contratación, selección, remuneraciones, desarrollo, control e incentivos del personal, así como sobre sanciones administrativas; V. Desarrollar los sistemas de premios, estímulos y recompensas, así como los reconocimientos que determinen las Condiciones Generales de Trabajo y las disposiciones jurídicas aplicables; VI. Conducir las relaciones laborales de la Coordinación, conforme a las disposiciones aplicables a los lineamientos que al efecto establezca el titular de la misma, así como supervisar y establecer lineamientos generales para las dependencias y entidades sectorizadas a la Coordinación; VII. Planear y conducir la política de desarrollo del personal, definir los puestos tipo y establecer los perfiles y requerimientos de los mismos, así como las formas de identificación del personal, y establecer políticas o lineamientos generales de aplicación en las dependencias y entidades sectorizadas a la Coordinación; XII. Fomentar la administración adecuada de los recursos humanos, materiales y tecnológicos en la Coordinación y en las dependencias y entidades sectorizadas a ésta; XIII. Establecer acciones para la adecuada administración de los recursos económicos, materiales y humanos en la Coordinación y en las dependencias y entidades sectorizadas a ésta; XVI. Acordar la liquidación y pago de cualquier remuneración al personal de la Coordinación; XXII. Elaborar y supervisar, en su ámbito de atribuciones, políticas de contratación del personal para el funcionamiento de la Coordinación y de las dependencias y entidades sectorizadas a la Coordinación; XXVI. Fungir como órgano de control disciplinario para la instauración del procedimiento administrativo de responsabilidad en contra de servidores públicos de la Coordinación, de conformidad a lo establecido en la Ley para los Servidores Públicos del Estado de Jalisco y sus Municipios, asesorando en su caso a las distintas áreas organizacionales en los asuntos relacionados con este tema;
Datos personales incluidos en el Sistema/Inventario:	
Inventario de datos personales:	
Tipo de tratamiento:	
Nivel de seguridad:	
Tiempo de resguardo de los datos personales:	

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

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:

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

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

La bitácora de acceso a los datos personales se utiliza sólo 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

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:

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

VIII. ANÁLISIS DE BRECHA

IX. GESTIÓN DE VULNERACIONES

El proceso es el siguiente:

FLUJOGRAMA	DETALLE NARRATIVO
 Inicio	
El área se percata de lo sucedido	
El área registra evento en bitácora de vulneraciones	

El área notifica a la Unidad de Transparencia sobre la eventualidad	
La UT registra en formato el evento	
La UT notifica mediante oficio al ITEI anexando el formato 6	
El responsable del área planea e implementa acciones preventivas y correctivas	
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 Seguridad realizará 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 seguimiento a la actualización del 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.

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.

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.
Visitas a las áreas una vez cada 6 meses	Verificar de primera mano la aplicación, actualización e impacto de las medidas de seguridad aplicadas. Verificar información en campo para determinar el grado de apego entre lo real y lo registrado en los sistemas de tratamiento.

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
Inducción en materia de transparencia y protección de datos personales	Enlaces de datos personales de la Coordinación General Estratégica de Seguridad	Concientizar al personal sobre la importancia de la protección de los datos personales	Unidad de Transparencia de la Coordinación General Estratégica de Seguridad y Secretaría de Seguridad	2019
Seminario de capacitaciones para enlaces de transparencia	Enlaces de datos personales de la Coordinación General Estratégica de Seguridad	Los asistentes deberán contar con los conocimientos sobre las disposiciones legales que señala la normatividad en datos personales	Coordinación General de Transparencia	2019
Medidas y controles de los datos personales	Enlaces de datos personales de la	Los asistentes deberán contar con el conocimiento	Coordinación General de Transparencia	2019

Tema	Asistentes	Objetivo	Facilitadores	Año
	Coordinación General Estratégica de Seguridad	necesario para la aplicación de medidas de seguridad físicas, administrativas y técnicas que protejan los datos personales		
• Clasificación y Desclasificación de la Información. • Información Confidencial. • Derecho a la Protección de Datos Personales	2 enlaces de las áreas administrativas de la Coordinación General Estratégica de Seguridad (Anexo 8, evidencia de la asistencia a la capacitación)	Contribuir al fortalecimiento de la cultura de la transparencia y protección de datos personales entre los Servidores Públicos del Estado de Jalisco, así como proporcionar herramientas Teórico-Conceptuales que permitan eficientar el cumplimiento de las disposiciones en la materia.	Personal de la Coordinación General de Transparencia	2020
Plataforma Nacional de Transparencia PNT	El enlace responsable de la actualización de la plataforma de transparencia y del SIPOT de la Coordinación General Estratégica de Seguridad. (Anexo 7, evidencia de la capacitación)	Reforzar conocimientos que ya tenemos, o en su caso, ayudar a unidades de transparencia o enlaces nuevos para que conozcan la PNT y la forma de cargar formatos	Personal del ITEI	2020
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 Coordinación General Estratégica de Seguridad	Que el personal se encuentre concientizado 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	2020
Versiones Públicas	Enlaces de datos personales de la Coordinación General Estratégica de Seguridad	Los asistentes contarán con habilidades para identificar información confidencial que se muestra en documentos, así como realizar versiones públicas para proteger la información	Unidad de Transparencia de la Coordinación General Estratégica de Seguridad y Secretaría de Seguridad	2021
Sensibilización de datos personales a personal operativo	Personal con funciones relacionadas con actividades operativas de la Coordinación General Estratégica de Seguridad	Los asistentes tomarán conciencia sobre las implicaciones del mal uso de los datos personales de terceras personas	Unidad de Transparencia de la Coordinación General Estratégica de Seguridad y Secretaría de Seguridad	2021