Documento de Seguridad
de la
Fiscalía Especializada en Combate a la Corrupción

Índice

Introducción

El presente Documento de Seguridad es de observancia obligatoria para los encargados y demás personas que realizan algún tipo de tratamiento de datos personales, dentro de la Fiscalía Especializada en Combate a la Corrupción (en lo sucesivo FECC); se elabora y aprueba en cumplimiento a lo dispuesto por los artículos 35 y 36 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios.

Tiene como objetivo describir y dar cuenta, de manera general, sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por la FECC para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee, de conformidad con la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios y demás disposiciones aplicables.

La información en posesión de la FECC, es un activo que debe ser protegido; ya que, por tratarse de información sensible, corre el riesgo de sufrir alguna vulneración a la privacidad y a la intimidad de las personas, quienes son los titulares de los datos personales que recaba, maneja y trata este sujeto obligado responsable. Por lo cual, de conformidad con la normatividad aplicable en la materia, es necesario crear sistemas y procesos que sean administrados por personal autorizado y capacitado.

De este modo, los mecanismos de gestión y administración de seguridad de la información, busca establecer procedimientos de operación y monitoreo, que tienen como fin mejorar los procesos en los que se involucran datos personales, aplicando sistemas de gestión y de seguridad, dando cumplimiento a la normatividad aplicable a la materia, así como los lineamientos y metodologías expedidos tanto por el órgano garante nacional, como el estatal; a efecto de estar en posibilidad de detectar las amenazas, establecer las medidas de seguridad pertinentes para reducir las posibles vulneraciones que pudieran existir y procurar la integridad, eficacia, confidencialidad y disponibilidad de los datos personales.

El Documento de Seguridad de la FECC, brinda homogeneidad los procesos que se llevan a cabo en la recolección de los datos personales, lo que permite que tanto el Comité de Transparencia, como la Unidad de Transparencia y los responsables de los sistemas, trabajen en conjunto para definir las medidas pertinentes de seguridad administrativas, físicas y técnicas con las que se cuenta para trabajar en la protección de los sistemas de datos personales, proporcionando mayor control y protección a los mismos.

Glosario

Áreas: Instancias de la FECC previstas en el reglamento interno, estatuto orgánico o instrumentos equivalentes, que cuentan o puedan contar, dar tratamiento, y ser responsables o encargadas de los datos personales;

Autenticidad: Busca asegurar la validez de la información en tiempo, forma y distribución. Así mismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades;

Autentificar: Acción de comprobar que la persona es quien dice ser;

Autorizar: Se considera como el acceso que se le permite a la persona que se ha identificado y autenticado apropiadamente. Esto depende del o de los permisos que le conceda el responsable de autorizar los accesos;

Aviso de privacidad: Documento físico, electrónico o en cualquier formato generado por el responsable, que es puesto a disposición del titular con el objeto de informarle los propósitos principales del tratamiento al que serán sometidos sus datos personales;

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

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

Clasificación: Acto por el cual se determina fundadamente que la información que posee la FECC es reservada o confidencial;

Cómputo en la nube: Modelo de provisión externa de servicios de cómputo bajo demanda que implica el suministro de infraestructura, plataforma o programa informático, distribuido de modo flexible, mediante procedimientos digitales, en recursos compartidos dinámicamente;

Confiabilidad de la información: Expresa la garantía de que la información generada es adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones;

Confidencialidad: Propiedad de prevenir la divulgación de información a personas o sistemas no autorizados, y que garantiza que la información sea accesible sólo a aquellas personas legamente facultadas o autorizadas para ello;

Consentimiento: Manifestación de la voluntad libre, específica e informada del titular que autoriza el tratamiento de sus datos personales sensibles;

Control de acceso: Medida de seguridad que permite el acceso únicamente a quien está autorizado para ello, una vez que se ha cumplido con el procedimiento de identificación y autentificación;

Datos personales: Cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información;

Datos personales sensibles: Aquellos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para este. De manera enunciativa, mas no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud, información genética, datos biométricos, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual;

Derechos ARCO: Los derechos de acceso, rectificación, cancelación y oposición al tratamiento de datos personales;

Disponibilidad: Característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones, garantizando el acceso a la información y a los recursos relacionados con la misma, cada vez que se requiera;

Documentos: Los expedientes, reportes, estudios, actas, resoluciones, oficios, correspondencia, acuerdos, directivas, directrices, circulares, contratos, convenios, instructivos, notas, memorandos, estadísticas, o bien, cualquier otro registro que documente el ejercicio de las facultades o la actividad de la FECC y sus servidores públicos, sin importar su fuente o fecha de elaboración. Los documentos podrán estar en cualquier medio existente, sea escrito, impreso, sonoro, visual, electrónico, informático u holográfico, o que se cree con posterioridad;

Encargado: Persona física o jurídica, pública o privada, ajena a la organización de la FECC, que sola o conjuntamente con otras, trata datos personales a nombre y por cuenta de la FECC;

Expediente: Un conjunto ordenado de documentos relacionados entre sí;

Información: El conjunto organizado de datos contenido en los documentos que la FECC genere, obtenga, adquiera, transforme o conserve por cualquier título;

Integridad: Es garantizar la exactitud, totalidad y la confiabilidad de la información y los sistemas o métodos de procesamiento de manera que éstos no puedan ser modificados sin autorización, ya sea accidental o intencionadamente;

Medidas compensatorias: Mecanismos alternos para dar a conocer a los titulares el aviso de privacidad, a través de su difusión por medios masivos de comunicación u otros de amplio alcance;

Medidas de seguridad: Conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permiten garantizar la protección, confidencialidad, disponibilidad e integridad de los datos personales;

Medidas de seguridad administrativas: 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, formación y capacitación del personal, en materia de protección de datos personales;

Medidas de seguridad físicas: Conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento.

Medidas de seguridad técnicas: Conjunto de acciones y mecanismos que se valen de la tecnología relacionada con hardware y software para proteger el entorno digital de los datos personales y recursos involucrados en su tratamiento.

Publicación: La difusión en medios electrónicos o impresos de información contenida en documentos;

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

Responsable Administrador: El servidor público titular de la unidad administrativa designado por el titular de la dependencia o entidad, que decide sobre el tratamiento físico o automatizado de datos personales, así como el contenido y finalidad de los sistemas de datos personales;

Responsable usuario: Los servidores públicos de la FECC que están autorizados para tratar datos personales;

Sistema de datos personales: El conjunto ordenado de datos personales que estén en posesión de un sujeto obligado;

Sistema de información: Se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales;

Soportes físicos: Son los medios de almacenamiento identificables a simple vista, que no requieren de ningún aparato que procese su contenido para examinar, modificar o

almacenar los datos; es decir, documentos, oficios, formularios impresos llenados “a mano” o “a máquina”, fotografías, placas radiológicas, carpetas, expedientes, entre otros;

Supresión: La baja archivística de los datos personales conforme a la normativa archivística aplicable, que resulte en la eliminación, borrado o destrucción de los datos personales bajo las medidas de seguridad previamente establecidas por el responsable;

Tecnología de la información: Se refiere al hardware y software operado por la FECC o por un tercero que procese información en su nombre, para llevar a cabo una función propia, sin tener en cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u otro tipo;

Titular: Persona física a quien pertenecen los datos personales;

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

Transmisión de datos personales. La entrega total o parcial de sistemas de datos personales a cualquier persona distinta del titular de los datos, mediante el uso de medios físicos o electrónicos tales como la interconexión de computadoras o bases de datos, acceso a redes de telecomunicación, así como a través de la utilización de cualquier otra tecnología que lo permita;

Transmisor: Dependencia o entidad que posee los datos personales objeto de la transmisión; y

Tratamiento: De manera enunciativa, mas no limitativa, cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados, aplicados a los datos personales, relacionadas con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales.

Abreviaturas

Comité: Comité de Transparencia de la Fiscalía Especializada en Combate a la Corrupción;

FECC: Fiscalía Especializada en Combate a la Corrupción;

ITEI: Instituto de Transparencia, Información Pública y Protección de Datos Personales del Estado de Jalisco;

INAI: Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales;

Ley: Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Jalisco y sus Municipios;

Ley de Transparencia: Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios;

Ley General: Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados;

Ley General de Transparencia: Ley General de Transparencia y Acceso a la Información Pública;

Plataforma Nacional: La Plataforma Nacional a la que hace referencia el artículo 49, de la Ley General de Transparencia;

Sistema Nacional: El Sistema Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales; y

Unidad: Unidad de Transparencia.

Marco Jurídico

Constitución Política de los Estados Unidos Mexicanos.

Constitución Política del Estado de Jalisco.

Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

Ley Orgánica de la Fiscalía del Estado de Jalisco.

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

Lineamientos para la Elaboración, Ejecución y Evaluación del Programa Nacional de Protección de Datos Personales.

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.

Sistemas de tratamiento o base de datos personales de la Fiscalía Especializada en Combate a la Corrupción

Cada uno de los Sistemas de Tratamiento de Datos Personales de conformidad con el artículo 36 de la Ley, contiene la siguiente información respecto a las siguientes fracciones:

I. El nombre de los sistemas de tratamiento o base de datos personales.

II. El nombre, cargo y adscripción del administrador de cada sistema de tratamiento.

III. Las funciones y obligaciones de las personas que traten datos personales.

Cabe señalar que, las funciones del administrador y usuario responsable que se consideraran, son las estrictamente concernientes al tratamiento de los datos personales o la finalidad para la cual fueron recabados.

De igual manera, las obligaciones que consideran son exclusivamente las tienen que ver con el tratamiento de datos personales.

IV. El inventario de los datos personales tratados.

V. La estructura y descripción de los sistemas de tratamiento de datos personales. señalando el tipo de soporte y las características del lugar donde se resguardan.

VI. Los controles y mecanismos de seguridad para las transferencias que, en su caso, se efectúen.

VII. El resguardo de los soportes físicos y/o electrónicos de los datos personales.

VIII. Las bitácoras de acceso, operación cotidiana y vulneraciones a la seguridad de los datos personales.

XI. La gestión de vulneraciones.

XII. Las medidas de seguridad físicas aplicadas a las instalaciones

XIII. Los controles de identificación y autenticación de usuarios.

XIV. Los procedimientos de respaldo y recuperación de datos personales.

XV. El plan de contingencia.

XVI. Las técnicas utilizadas para la supresión y borrado seguro de los datos personales.

Ejercicio de Derecho de Petición

<table>
<tr><th colspan="8">Unidad Administrativa: Oficialía de Partes</th></tr>
<tr><td colspan="2">I.- Nombre del sistema:</td><td colspan="6">Ejercicio de Derecho de Petición</td></tr>
<tr><td colspan="8">II.- Nombre cargo y adscripción del administrador del sistema.
III.- Funciones y obligaciones de las personas que traten datos personales.</td></tr>
<tr><td colspan="8">Administrador Responsable</td></tr>
<tr><td>Nombre:</td><td colspan="3">María Eugenia Flores Chávez</td><td>Cargo:</td><td colspan="3">Secretaria Particular</td></tr>
<tr><td colspan="8">Funciones:
Brindar atención a los ciudadanos que acudan a externar sus quejas y peticiones, así como canalizarlos a las áreas correspondientes y dar el debido el seguimiento a las mismas.
Proporcionar a los ciudadanos una información correcta y adecuada de los trámites y servicios de la Dependencia cuando así lo soliciten.
Establecer los mecanismos que permitan guardar la confidencialidad de la información que se genere en su área, así como la que se tiene archivada, de conformidad con la legislación aplicable
Instruir el establecimiento de los parámetros y medidas de seguridad que debe contener el Sistema.</td></tr>
<tr><td colspan="8">Obligaciones:
Proteger los datos personales que tenga en su posesión.
Tratar los de datos personales cuando sea exclusivamente en observancia a las facultades o atribuciones a la normatividad aplicable.
Vigilar y supervisar que se lleve a cabo el correcto resguardo de datos personales.</td></tr>
<tr><td colspan="8">Encargado</td></tr>
<tr><td colspan="2">Nombre:</td><td colspan="2">No aplica</td><td>Cargo:</td><td colspan="3">No aplica</td></tr>
<tr><td colspan="8">Funciones y Obligaciones: No aplica</td></tr>
<tr><td colspan="8">IV.- Inventario de datos personales
V.- Estructura y descripción de los sistemas</td></tr>
<tr><td colspan="2">Ordinarios:</td><td colspan="6">Identificativos: Nombre, domicilio, número de identificación, firma.</td></tr>
<tr><td colspan="2">Sensibles:</td><td colspan="6">No aplica</td></tr>
<tr><td colspan="2">Quién suministra</td><td colspan="6">De forma personal, directamente del titular</td></tr>
<tr><td colspan="2">Cómo suministra</td><td colspan="6">Formato físico</td></tr>
<tr><td colspan="2">Finalidad:</td><td colspan="6">Dar respuesta a las peticiones que realizan los ciudadanos a la FECC y/o a su Titular.</td></tr>
<tr><td colspan="2" rowspan="3">Tipo de Soporte</td><td>Físico</td><td>Sí</td><td>Electrónico</td><td>No</td><td>Otro:</td><td>No</td></tr>
<tr><td>Descripción</td><td colspan="5">Físico: Expediente numerado de la petición.</td></tr>
<tr><td>Características del lugar donde se resguardan</td><td colspan="5">Archivero y Computadora</td></tr>
<tr><td colspan="2">Participación en el ciclo de vida del dato personal</td><td colspan="6">Obtención, conservación y almacenamiento.</td></tr>
<tr><td colspan="8">VI.- Controles y Mecanismos de Seguridad de las transferencias
VII.- Resguardo de los Sistemas
VIII.- Bitácoras para accesos y operación cotidiana
XII.- Medidas de seguridad aplicadas a las instalaciones
XIII.- Controles de identificación y autenticación de los usuarios</td></tr>
<tr><td colspan="2">Nivel de seguridad</td><td>Básico</td><td>x</td><td>Medio</td><td></td><td>Alto</td><td></td></tr>
<tr><td colspan="8">Transferencias de datos personales</td></tr>
<tr><td colspan="2" rowspan="3">Transferencia Electrónico y digital:</td><td>Web service</td><td>No aplica</td><td>Web Transfer</td><td>No aplica</td><td>Nube</td><td>No aplica</td></tr>
<tr><td>Discos externos</td><td>No aplica</td><td>Carpetas compartidas</td><td>No aplica</td><td>CD</td><td>No aplica</td></tr>
<tr><td>Correo</td><td>No aplica</td><td>USB</td><td>No aplica</td><td>Otro:</td><td>No aplica</td></tr>
<tr><td colspan="2">Medidas de seguridad transferencia electrónica digital</td><td colspan="6">No aplica</td></tr>
<tr><td colspan="2">Transferencia Físico</td><td colspan="6">No aplica</td></tr>
<tr><td colspan="2">Medidas de seguridad transferencia física</td><td colspan="6">No aplica</td></tr>
<tr><td colspan="8">Almacenamiento Sistemas de Datos Personales</td></tr>
</table>

Almacenamiento Electrónico y digital:	**Servidor**	No aplica	**Computadora**	no aplica	**Nube**	No aplica
	Discos externos	No aplica	**Carpetas compartidas**	No aplica	**CD**	No aplica
	Correo	No aplica	**USB**	No aplica	**Otro:**	No aplica
Medidas de seguridad almacenamiento electrónica digital	Sistema de firewall, antivirus, contraseñas para acceder a las computadoras, sistemas de bloqueo de pantalla cada 5 minutos en las computadoras					
Almacenamiento Físico	Expedientes consecutivos					
Medidas de seguridad almacenamiento física	Archiveros y puertas con chapa para accesar a los mismos.					
Acceso a las instalaciones						
Seguridad perimetral exterior: Resguardo policial, cámaras de seguridad y puerta con llave.						
Seguridad perimetral interior: Puerta con llave						
Bitácoras para accesos y operación cotidiana						
Los datos que se registran en las bitácoras: No aplica.						
Soporte de la bitácora:	**Físico**		**Electrónico**		**Otro:**	
Lugar de almacenamiento:				**Tiempo**		
Como se asegura la integridad:						
XI.- Gestión de Vulneraciones						
Datos que se registran: No aplica						
Soporte del registro:	**Físico**		**Electrónico**		**Otro:**	
Lugar de almacenamiento:				**Tiempo**		
Como se asegura la integridad:						
XIV.- Respaldo y recuperación de datos						
Tipo de respaldo:	**Completo**		**Diferencial**		**Incremental**	
Medios para almacenar copias de seguridad	Registro único					
XV.- Plan de Contingencia						
Se cuenta con Plan de contingencia			Si		No	x
Se realizan pruebas de eficiencia			Si		No	x
Se cuenta con un sitio redundante			Si		No	x
Tipo de sitio :	**Caliente**	No aplica	**Tibio**	No aplica	**Frío**	No aplica
	Propio	No aplica	**Subcontratado**	No aplica	**Tiempo**	No aplica
Procedimiento	No aplica					
Equipo	No aplica					
Personal	No aplica					
XVI.- Técnicas para la supresión y borrado seguro de los datos personales						
Datos del sistema que será cancelado: No aplica						
Denominación:	No aplica					
Motivos:	No aplica					
Plazos y condiciones para el bloqueo del sistema: No aplica						
Medidas de seguridad para el bloqueo y posterior supresión del sistema: No aplica						
Procedimiento para la supresión y período de conservación del sistema: No aplica						
Mecanismos para la supresión del sistema: No aplica						

Registro de Visitas

<table>
<tr><th colspan="8">Unidad Administrativa: Oficialía de Partes</th></tr>
<tr><td colspan="2">I.- Nombre del sistema:</td><td colspan="6">Registro de Visitas</td></tr>
<tr><td colspan="8">II.- Nombre cargo y adscripción del administrador del sistema
III.- Funciones y obligaciones de las personas que traten datos personales.</td></tr>
<tr><td colspan="8">Administrador Responsable</td></tr>
<tr><td>Nombre:</td><td colspan="3">Felipa Reyes Jiménez</td><td>Cargo:</td><td colspan="3">Encargada de Área C</td></tr>
<tr><td colspan="8">Funciones:
Brindar atención a los ciudadanos que acudan a externar sus quejas y peticiones, así como canalizarlos a las áreas correspondientes y dar el debido seguimiento a las mismas.
Resguardar el registro de visitas de la FECC.
Instruir el cumplimiento y seguimiento del sistema de datos personales denominado Registro de visitas.
Establecer los mecanismos de control que aseguren la administración óptima y la adecuada operación del Registro de visitas.
Instruir el establecimiento de los parámetros y medidas de seguridad que debe contener el Sistema.</td></tr>
<tr><td colspan="8">Obligaciones:
Proteger los datos personales que tenga en su posesión.
Tratar los de datos personales cuando sea exclusivamente en observancia a las facultades o atribuciones a la normatividad aplicable.
Vigilar y supervisar que se lleve a cabo el correcto resguardo de datos personales.</td></tr>
<tr><td colspan="8">Encargado</td></tr>
<tr><td colspan="2">Nombre:</td><td colspan="2">No aplica</td><td>Cargo:</td><td colspan="3">No aplica</td></tr>
<tr><td colspan="8">Funciones y Obligaciones: No aplica</td></tr>
<tr><td colspan="8">IV.- Inventario de datos personales
V.- Estructura y descripción de los sistemas</td></tr>
<tr><td>Ordinarios:</td><td colspan="7">Identificativos: Nombre, número de identificación, firma.</td></tr>
<tr><td>Sensibles:</td><td colspan="7">No aplica</td></tr>
<tr><td colspan="2">Quién suministra</td><td colspan="6">De forma personal, directamente del titular</td></tr>
<tr><td colspan="2">Cómo suministra</td><td colspan="6">Formato físico</td></tr>
<tr><td colspan="2">Finalidad:</td><td colspan="6">Llevar un registro de las personas que ingresan a las instalaciones de la FECC, para estadísticas y control.</td></tr>
<tr><td colspan="2" rowspan="3">Tipo de Soporte</td><td>Físico</td><td>Sí</td><td>Electrónico</td><td>No</td><td>Otro:</td><td>No</td></tr>
<tr><td>Descripción</td><td colspan="5">Físico: Libro de registro</td></tr>
<tr><td>Características del lugar donde se resguardan</td><td colspan="5">Recepción y Archivero</td></tr>
<tr><td colspan="2">Participación en el ciclo de vida del dato personal</td><td colspan="6">Obtención, conservación y almacenamiento.</td></tr>
<tr><td colspan="8">VI.- Controles y Mecanismos de Seguridad de las transferencias
VII.- Resguardo de los Sistemas
VIII.- Bitácoras para accesos y operación cotidiana
XII.- Medidas de seguridad aplicadas a las instalaciones
XIII.- Controles de identificación y autenticación de los usuarios</td></tr>
<tr><td colspan="2">Nivel de seguridad</td><td>Básico</td><td>x</td><td>Medio</td><td></td><td>Alto</td><td></td></tr>
<tr><td colspan="8">Transferencias de datos personales</td></tr>
<tr><td colspan="2" rowspan="3">Transferencia Electrónico y digital:</td><td>Web service</td><td>No aplica</td><td>Web Transfer</td><td>No aplica</td><td>Nube</td><td>No aplica</td></tr>
<tr><td>Discos externos</td><td>No aplica</td><td>Carpetas compartidas</td><td>No aplica</td><td>CD</td><td>No aplica</td></tr>
<tr><td>Correo</td><td>No aplica</td><td>USB</td><td>No aplica</td><td>Otro:</td><td>No aplica</td></tr>
<tr><td colspan="2">Medidas de seguridad transferencia electrónica digital</td><td colspan="6">No aplica</td></tr>
<tr><td colspan="2">Transferencia Físico</td><td colspan="6">No aplica</td></tr>
<tr><td colspan="2">Medidas de seguridad transferencia física</td><td colspan="6">No aplica</td></tr>
</table>

Almacenamiento Sistemas de Datos Personales						
Almacenamiento Electrónico y digital:	**Servidor**	No aplica	**Computadora**	no aplica	**Nube**	No aplica
	Discos externos	No aplica	**Carpetas compartidas**	No aplica	**CD**	No aplica
	Correo	No aplica	**USB**	No aplica	**Otro:**	No aplica
Medidas de seguridad almacenamiento electrónica digital	No aplica					
Almacenamiento Físico	Libro de registro sobre mueble en recepción y archivero.					
Medidas de seguridad almacenamiento física	Puertas con chapa para accesar a la FECC con seguridad a la entrada e ingreso controlado.					
Acceso a las instalaciones						
Seguridad perimetral exterior: Resguardo policial, cámaras de seguridad y puerta con llave.						
Seguridad perimetral interior: Puerta con llave						
Bitácoras para accesos y operación cotidiana						
Los datos que se registran en las bitácoras: No aplica.						
Soporte de la bitácora:	**Físico**		**Electrónico**		**Otro:**	
Lugar de almacenamiento:				**Tiempo**		
Como se asegura la integridad:						
XI.- Gestión de Vulneraciones						
Datos que se registran: No aplica						
Soporte del registro:	**Físico**		**Electrónico**		**Otro:**	
Lugar de almacenamiento:				**Tiempo**		
Como se asegura la integridad:						
XIV.- Respaldo y recuperación de datos						
Tipo de respaldo:	**Completo**		**Diferencial**		**Incremental**	
Medios para almacenar copias de seguridad	Registro único					
XV.- Plan de Contingencia						
Se cuenta con Plan de contingencia			Si		No	x
Se realizan pruebas de eficiencia			Si		No	x
Se cuenta con un sitio redundante			Si		No	x
Tipo de sitio :	**Caliente**	No aplica	**Tibio**	No aplica	**Frío**	No aplica
	Propio	No aplica	**Subcontratado**	No aplica	**Tiempo**	No aplica
Procedimiento	No aplica					
Equipo	No aplica					
Personal	No aplica					
XVI.- Técnicas para la supresión y borrado seguro de los datos personales						
Datos del sistema que será cancelado: No aplica						
Denominación:	No aplica					
Motivos:	No aplica					
Plazos y condiciones para el bloqueo del sistema: No aplica						
Medidas de seguridad para el bloqueo y posterior supresión del sistema: No aplica						
Procedimiento para la supresión y período de conservación del sistema: No aplica						
Mecanismos para la supresión del sistema: No aplica						

Registro de Documentos Recibidos

<table>
<tr><th colspan="8">Unidad Administrativa: Oficialía de Partes</th></tr>
<tr><td colspan="2">I.- Nombre del sistema:</td><td colspan="6">Registro de Documentos Recibidos</td></tr>
<tr><td colspan="8">II.- Nombre cargo y adscripción del administrador del sistema
III.- Funciones y obligaciones de las personas que traten datos personales.</td></tr>
<tr><td colspan="8">Administrador Responsable</td></tr>
<tr><td>Nombre:</td><td colspan="3">Felipa Reyes Jiménez</td><td>Cargo:</td><td colspan="3">Encargada de Área C</td></tr>
<tr><td colspan="8">Funciones:
Recibir la correspondencia dirigida a la FECC, al Fiscal Especializado, así como de aquellas áreas administrativas y sus titulares.
Revisar la correspondencia presentada, acusando de recibo a los particulares en las copias y duplicados que les presenten, asentando fecha, hora y documentación anexa.
Mantener bajo su cuidado los promociones, oficios, denuncias y en general todos los documentos recibidos hasta en tanto se entreguen a las áreas administrativas correspondientes para dar trámite a los mismos.
Turnar a las áreas administrativas competentes la correspondencia y los anexos que en su caso se presenten para el trámite y seguimiento de la documentación.
Tener a su cargo y bajo su responsabilidad los libros de registro de la documentación recibida en donde se señale el destino de la documentación, para el control y estadística de la documentación recibida.
Instruir el cumplimiento y seguimiento del sistema de datos personales denominado Registro de Documentos Recibidos.
Establecer los mecanismos de control que aseguren la administración óptima y la adecuada operación del Registro de Documentos Recibidos.
Instruir el establecimiento de los parámetros y medidas de seguridad que debe contener el Sistema.</td></tr>
<tr><td colspan="8">Obligaciones:
Proteger los datos personales que tenga en su posesión.
Tratar los de datos personales cuando sea exclusivamente en observancia a las facultades o atribuciones a la normatividad aplicable.
Vigilar y supervisar que se lleve a cabo el correcto resguardo de datos personales.</td></tr>
<tr><td colspan="8">Encargado</td></tr>
<tr><td colspan="2">Nombre:</td><td colspan="2">No aplica</td><td>Cargo:</td><td colspan="3">No aplica</td></tr>
<tr><td colspan="8">Funciones y Obligaciones: No aplica</td></tr>
<tr><td colspan="8">IV.- Inventario de datos personales
V.- Estructura y descripción de los sistemas</td></tr>
<tr><td>Ordinarios:</td><td colspan="7">Identificativos: Nombre del remitente y ocasionalmente algún dato adicional.</td></tr>
<tr><td>Sensibles:</td><td colspan="7">No aplica</td></tr>
<tr><td colspan="2">Quién suministra</td><td colspan="6">De forma personal y directamente del titular</td></tr>
<tr><td colspan="2">Cómo suministra</td><td colspan="6">Formato físico</td></tr>
<tr><td>Finalidad:</td><td colspan="7">Llevar un registro de documentos (denuncias, promociones, y oficios) recibidos en la FECC</td></tr>
<tr><td rowspan="3">Tipo de Soporte</td><td>Físico</td><td>Sí</td><td>Electrónico</td><td>No</td><td>Otro:</td><td colspan="2">No</td></tr>
<tr><td>Descripción</td><td colspan="5">Físico: Libro de registro</td></tr>
<tr><td>Características del lugar donde se resguardan</td><td colspan="5">Archivero</td></tr>
<tr><td colspan="2">Participación en el ciclo de vida del dato personal</td><td colspan="6">Obtención, conservación y almacenamiento.</td></tr>
<tr><td colspan="8">VI.- Controles y Mecanismos de Seguridad de las transferencias
VII.- Resguardo de los Sistemas
VIII.- Bitácoras para accesos y operación cotidiana
XII.- Medidas de seguridad aplicadas a las instalaciones
XIII.- Controles de identificación y autenticación de los usuarios</td></tr>
<tr><td colspan="2">Nivel de seguridad</td><td>Básico</td><td>x</td><td>Medio</td><td></td><td>Alto</td><td></td></tr>
<tr><td colspan="8">Transferencias de datos personales</td></tr>
<tr><td rowspan="3">Transferencia Electrónico y digital:</td><td>Web service</td><td>No aplica</td><td>Web Transfer</td><td>No aplica</td><td>Nube</td><td colspan="2">No aplica</td></tr>
<tr><td>Discos externos</td><td>No aplica</td><td>Carpetas compartidas</td><td>No aplica</td><td>CD</td><td colspan="2">No aplica</td></tr>
<tr><td>Correo</td><td>No aplica</td><td>USB</td><td>No aplica</td><td>Otro:</td><td colspan="2">No aplica</td></tr>
</table>

Medidas de seguridad transferencia electrónica digital	No aplica					
Transferencia Físico	No aplica					
Medidas de seguridad transferencia física	No aplica					
Almacenamiento Sistemas de Datos Personales						
Almacenamiento Electrónico y digital:	**Servidor**	No aplica	**Computadora**	No aplica	**Nube**	No aplica
	Discos externos	No aplica	**Carpetas compartidas**	No aplica	**CD**	No aplica
	Correo	No aplica	**USB**	No aplica	**Otro:**	No aplica
Medidas de seguridad almacenamiento electrónica digital	No aplica					
Almacenamiento Físico	Archivero					
Medidas de seguridad almacenamiento física	Puertas con chapa para accesar a la FECC con seguridad a la entrada e ingreso controlado.					
Acceso a las instalaciones						
Seguridad perimetral exterior: Resguardo policial, cámaras de seguridad y puerta con llave						
Seguridad perimetral interior: Puerta con llave						
Bitácoras para accesos y operación cotidiana						
Los datos que se registran en las bitácoras: No aplica.						
Soporte de la bitácora:	**Físico**		**Electrónico**		**Otro:**	
Lugar de almacenamiento:				**Tiempo**		
Como se asegura la integridad:						
XI.- Gestión de Vulneraciones						
Datos que se registran: No se tiene						
Soporte del registro:	**Físico**		**Electrónico**		**Otro:**	
Lugar de almacenamiento:				**Tiempo**		
Como se asegura la integridad:	No aplica					
XIV.- Respaldo y recuperación de datos						
Tipo de respaldo:	**Completo**		**Diferencial**		**Incremental**	
Medios para almacenar copias de seguridad	Registro único					
XV.- Plan de Contingencia						
Se cuenta con Plan de contingencia			Si		No	x
Se realizan pruebas de eficiencia			Si		No	x
Se cuenta con un sitio redundante			Si		No	x
Tipo de sitio :	**Caliente**	No aplica	**Tibio**	No aplica	**Frío**	No aplica
	Propio	No aplica	**Subcontratado**	No aplica	**Tiempo**	No aplica
Procedimiento	No aplica					
Equipo	No aplica					
Personal	No aplica					
XVI.- Técnicas para la supresión y borrado seguro de los datos personales						
Datos del sistema que será cancelado: No aplica						
Denominación:	No aplica					
Motivos:	No aplica					
Plazos y condiciones para el bloqueo del sistema: No aplica						
Medidas de seguridad para el bloqueo y posterior supresión del sistema: No aplica						
Procedimiento para la supresión y período de conservación del sistema: No aplica						
Mecanismos para la supresión del sistema: No aplica						

Integración de Carpetas de Investigación

<table>
<tr><th colspan="4">UNIDAD ADMINISTRATIVA: Dirección de Control de Procesos y Audiencias de las Agencias del Ministerio Público.</th></tr>
<tr><td colspan="2">I.- Nombre del sistema:</td><td colspan="2">Integración de Carpetas de Investigación</td></tr>
<tr><td colspan="4">II.- Nombre cargo y adscripción del administrador del sistema
III.- funciones y obligaciones de las personas que traten datos personales.</td></tr>
<tr><td colspan="4">Administrador Responsable</td></tr>
<tr><td>Nombre:</td><td>Director de Control de Procesos y Audiencias de las Agencias del Ministerio Público.</td><td>Cargo:</td><td>Director de Control de Procesos y Audiencias de las Agencias del Ministerio Público.</td></tr>
<tr><td colspan="4">Funciones:
Contribuir en la organización, coordinación y supervisión de las actividades de los Agentes del Ministerio público adscritos a los Juzgados Penales y Especializados.
Intervenir en los procesos penales de primera instancia cuya atención y tramitación le corresponda en los términos de ley, además de aportar las pruebas pertinentes y promover las diligencias orientadas al debido esclarecimiento de los hechos, así como para la acreditación del cuerpo del delito, la responsabilidad penal de los inculpados y la relativa a la reparación de los daños.
Interponer cuando así proceda los recursos pertinentes establecidos por la ley.
Formular conclusiones en los términos señalados por la ley y solicitar la imposición de las penas y medidas de seguridad que correspondan y el pago de la reparación del daño.
Solicitar las ordenes de aprehensión en los términos de la Constitución de los Estados Unidos Mexicanos solicitar las medidas precautorias de arraigo o las órdenes de cateo necesarias.
Solicitar por conducto de los agentes del Ministerio Público adscritos a los órganos jurisdiccionales las órdenes de aseguramiento precautorio de bienes para los efectos de pago de la reparación de los daños y perjuicios ocasionados por la comisión de delitos.
Y las demás que le sean asignadas por el Fiscal Especializado en Combate a la Corrupción.
Instruir el cumplimiento y seguimiento del sistema de datos personales denominado Integración de Carpetas de Investigación.
Establecer los mecanismos de control que aseguren la administración óptima y la adecuada operación del Integración de Carpetas de Investigación.
Instruir el establecimiento de los parámetros y medidas de seguridad que debe contener el Sistema.</td></tr>
<tr><td colspan="4">Obligaciones:
Proteger los datos personales en posesión.
Tratar los de datos personales cuando sea exclusivamente en observancia a las facultades o atribuciones a la normatividad aplicable.
Vigilar y supervisar que se lleve a cabo el correcto resguardo de datos personales.</td></tr>
<tr><td colspan="4">Usuario Responsable 1</td></tr>
<tr><td>Nombre:</td><td>Agente Especializado del Ministerio Público</td><td>Cargo:</td><td>Agente Especializado del Ministerio Público</td></tr>
</table>

Funciones:

- Actuar en estricto apego a los principios de legalidad, objetividad, eficiencia, profesionalismo y honradez, así como vigilar que en toda investigación de los delitos se cumpla estrictamente con los derechos humanos reconocidos en la legislación aplicable.
- Recibir las denuncias o querellas que le presenten en forma oral, por escrito, o a través de medios digitales, incluso mediante denuncias anónimas en términos de las disposiciones legales aplicables, sobre hechos que puedan constituir algún delito.
- Ejercer el control, la conducción y el mando de la investigación de los delitos que atiende la agencia especializada, para lo cual deberá coordinar a las Policías y a los peritos durante la misma.
- Ordenar o supervisar, según sea el caso, la aplicación y ejecución de las medidas necesarias para impedir que se pierdan, destruyan o alteren los indicios, una vez que tenga noticia del mismo, cerciorándose de que se han seguido las reglas y protocolos para su preservación y procesamiento; por lo cual deberá instruir a las Policías sobre la legalidad, pertinencia, suficiencia y contundencia de los indicios recolectados o por recolectar, así como las demás actividades y diligencias que deben ser llevadas a cabo dentro de la investigación.
- Iniciar la investigación de delitos especializados correspondiente cuando así proceda y, en su caso, ordenar la recolección de indicios y medios de prueba que deberán servir para sus respectivas resoluciones y las del Órgano jurisdiccional, así como recabar los elementos necesarios que determinen el daño causado por el delito y la cuantificación del mismo para los efectos de su reparación.
- Ejercer funciones de investigación respecto de los delitos en materias concurrentes, cuando ejerza la facultad de atracción y en los demás casos que las leyes lo establezcan.
- Ordenar a la Policía y a sus auxiliares, en el ámbito de su competencia, la práctica de actos de investigación conducentes para el esclarecimiento del hecho delictivo, así como analizar las que dichas autoridades hubieren practicado, supervisando y controlando cada una de las acciones realizadas.
- Requerir informes o documentación a otras autoridades y a particulares, así como solicitar la práctica de peritajes y diligencias para la obtención de otros medios de prueba.
- Solicitar al Órgano jurisdiccional la autorización de actos de investigación y demás actuaciones que sean necesarias dentro de la misma.
- Ordenar la detención y la retención de los imputados cuando resulte procedente en los términos que se establecen las leyes y código aplicables; así como Ejercer la acción penal cuando proceda.
- Brindar las medidas de seguridad necesarias, a efecto de garantizar que las víctimas u ofendidos o testigos del delito puedan llevar a cabo la identificación del imputado sin riesgo para ellos; así como promover las acciones necesarias para que se provea la seguridad y proporcionar el auxilio a víctimas, ofendidos, testigos, jueces, magistrados, agentes del Ministerio Público, Policías, peritos y, en general, a todos los sujetos que con motivo de su intervención en el procedimiento, cuya vida o integridad corporal se encuentren en riesgo inminente.
- Determinar el archivo temporal y el no ejercicio de la acción penal, así como ejercer la facultad de no investigar en los casos autorizados por este Código.
- Poner a disposición del Órgano jurisdiccional a las personas detenidas dentro de los plazos establecidos en el presente Código.
- Solicitar las medidas cautelares aplicables al imputado en el proceso, en atención a las disposiciones conducentes y promover su cumplimiento.
- Comunicar al Órgano jurisdiccional y al imputado los hechos, así como los datos de prueba que los sustentan y la fundamentación jurídica, atendiendo al objetivo o finalidad de cada etapa del procedimiento.
- Solicitar a la autoridad judicial la imposición de las penas o medidas de seguridad que correspondan.
- Solicitar el pago de la reparación del daño a favor de la víctima u ofendido del delito, sin perjuicio de que éstos lo pudieran solicitar directamente.
- Las demás que señalen la legislación vigente y otras disposiciones aplicables.
- Realizar el debido manejo de la información que integra el Sistema de Integración de Carpetas de Investigación.

Obligaciones:

- Proteger los datos personales en posesión.
- Tratar los de datos personales cuando sea exclusivamente en observancia a las facultades o atribuciones a la normatividad aplicable.
- Mantener la integridad, disponibilidad y confidencialidad de la información; así como dar cumplimiento a las medidas de seguridad.

Usuario Responsable 2			
Nombre:	Secretario Especializado de la Agencia del Ministerio Público	**Cargo**:	Secretario Especializado de la Agencia del Ministerio Público

Funciones:

- Auxiliar desde ámbito de su competencia al Agente Especializado del Ministerio Público en cada una de las actuaciones dentro de la investigación que prevea la legislación y normatividad aplicable y vigente.
- Ejecutar por orden el Agente Especializado del Ministerio Público y en el ámbito de su competencia, la práctica de actos de investigación conducentes para el esclarecimiento del hecho delictivo, así como analizar las que dichas autoridades hubieren practicado.
- Apoyar en las audiencias conciliatorias que se llevan a cabo en la dependencia.
- Auxiliar al Agente Especializado del Ministerio Público en la formulación de agravios y/o desistimientos ante la segunda instancia.
- Ayudar en la integración de la carpeta de investigación.
- Y demás actividades contempladas en la normatividad vigente.
- Realizar el debido manejo de la información que alimenta el Sistema de Integración de Carpetas de Investigación

Obligaciones:

- Proteger los datos personales en posesión.
- Tratar los de datos personales cuando sea exclusivamente en observancia a las facultades o atribuciones a la normatividad aplicable.
- Mantener la integridad, disponibilidad y confidencialidad de la información; así como dar cumplimiento a las medidas de seguridad.

Usuario Responsable 3			
Nombre:	Actuario Especializado del Ministerio Público	**Cargo**:	Actuario Especializado del Ministerio Público

Funciones:

- Auxiliar desde el ámbito de su competencia al Ministerio Público en todas las actividades que resulten necesarias para la Procuración de Justicia, a fin de brindar seguimiento administrativo.
- Levantar denuncias por comparecencia.
- Solicitar informes a diferentes dependencias por medio de oficio.
- Citar a diferentes personas que tengan que declarar, respecto de la carpeta de investigación que se está integrando.
- Y demás actividades contempladas en la normatividad vigente y aplicable.
- Realizar el debido manejo de la información que alimenta el Sistema de Integración de Carpetas de Investigación

Obligaciones:

- Proteger los datos personales en posesión.
- Tratar los de datos personales cuando sea exclusivamente en observancia a las facultades o atribuciones a la normatividad aplicable.
- Mantener la integridad, disponibilidad y confidencialidad de la información; así como dar cumplimiento a las medidas de seguridad.

Usuario Responsable 4			
Nombre:	Policía Investigador	**Cargo**:	Policía Investigador

Funciones:

- Coordinarse con las Agencias del Ministerio Público en la realización de investigaciones, aseguramiento de bienes y demás diligencias en las que él y sus subalternos actúan bajo el mando del titular de dichas instancias, reportando a este último cada una de sus actuaciones.
- Acudir al lugar de los hechos en donde se cometió un delito, realizar entrevista de testigos presenciales, recabar pruebas o vestigios con relación a los mismos.
- Asignar y supervisar el trabajo de investigación, operativos y demás tareas inherentes al área.
- Auxiliar en las investigaciones, presentaciones, localizaciones, identificaciones y detenciones ordenadas por las agencias del Ministerio Público.
- Recibir las denuncias escritas, verbales y anónimas sobre hechos que puedan ser constitutivos de delito e informar al Ministerio Público por cualquier medio y de forma inmediata de las diligencias practicadas.
- Realizar detenciones en los casos que autoriza la Constitución, haciendo saber a la persona detenida los derechos que ésta le otorga;
- Impedir que se consumen los delitos o que los hechos produzcan consecuencias ulteriores. Especialmente estará obligada a realizar todos los actos necesarios para evitar una agresión real, actual o inminente y sin derecho en protección de bienes jurídicos de los gobernados a quienes tiene la obligación de proteger.
- Requerir a las autoridades competentes y solicitar a las personas físicas o morales, informes y documentos para fines de la investigación. En caso de negativa, informará al Ministerio Público para que determine lo conducente.
- Proporcionar atención a víctimas u ofendidos o testigos del delito de acuerdo a protocolos, normatividad y legislación vigente y aplicable.
- Emitir el informe policial y demás documentos, de conformidad con las disposiciones aplicables. Para tal efecto se podrá apoyar en los conocimientos que resulten necesarios, sin que ello tenga el carácter de informes periciales, y
- Las demás que le confieran la legislación vigente y otras disposiciones aplicables.
- Realizar el debido manejo de la información que alimenta el Sistema de Integración de Carpetas de Investigación

Obligaciones:

- Proteger los datos personales en posesión.
- Tratar los de datos personales cuando sea exclusivamente en observancia a las facultades o atribuciones a la normatividad aplicable.
- Mantener la integridad, disponibilidad y confidencialidad de la información; así como dar cumplimiento a las medidas de seguridad.

Usuario Responsable 5

Nombre:	Policía Investigador B	**Cargo**:	Policía Investigador B

Funciones:

- Realizar investigaciones, presentaciones, localizaciones e identificaciones de probables responsables de un delito, en auxilio y bajo el mando del Ministerio Público, informando y recibiendo instrucción de éste último en cada una de sus actuaciones.
- Cumplimentar los Mandamientos Judiciales y demás diligencias, ordenadas por la autoridad competente y superiores.
- Acudir al lugar de los hechos en donde se cometió un delito, realizar operativos consistentes en entrevistas de testigos presenciales, recabar pruebas o vestigios con relación a los mismos, o la detención de un presunto responsable de acuerdo a normatividad aplicable.
- Recibir las denuncias escritas, verbales y anónimas sobre hechos que puedan ser constitutivos de delito e informar al Ministerio Público por cualquier medio y de forma inmediata de las diligencias practicadas.
- Realizar detenciones en los casos que autoriza la Constitución, haciendo saber a la persona detenida los derechos que ésta le otorga;
- Impedir que se consumen los delitos o que los hechos produzcan consecuencias ulteriores. Especialmente estará obligada a realizar todos los actos necesarios para evitar una agresión real, actual o inminente y sin derecho en protección de bienes jurídicos de los gobernados a quienes tiene la obligación de proteger.
- Requerir a las autoridades competentes y solicitar a las personas físicas o morales, informes y documentos para fines de la investigación. En caso de negativa, informará al Ministerio Público para que determine lo conducente
- Proporcionar atención a víctimas u ofendidos o testigos del delito de acuerdo a protocolos, normatividad y legislación vigente y aplicable.
- Emitir el informe policial y demás documentos, de conformidad con las disposiciones aplicables. Para tal efecto se podrá apoyar en los conocimientos que resulten necesarios, sin que ello tenga el carácter de informes periciales.
- Las demás que le confieran la legislación vigente y otras disposiciones aplicables.

• Realizar el debido manejo de la información que alimentar el Sistema de Integración de Carpetas de Investigación.						
Obligaciones: • Proteger los datos personales en posesión. • Tratar los de datos personales cuando sea exclusivamente en observancia a las facultades o atribuciones a la normatividad aplicable. • Mantener la integridad, disponibilidad y confidencialidad de la información; así como dar cumplimiento a las medidas de seguridad.						
Encargado						
Nombre:	No aplica		**Cargo**:	No aplica		
Funciones y Obligaciones: No aplica						
IV.- Inventario de datos personales **V.- Estructura y descripción de los sistemas**						
Ordinarios:	Identificativos: Nombre, estado civil, edad, fecha de nacimiento, lugar de nacimiento, sexo, nacionalidad, ocupación, nivel académico, domicilio particular y en su caso laboral, número de teléfono, identificación oficial, correo electrónico, entre otros. Patrimoniales: descripción o documentación que acredite la posesión o propiedad de bienes muebles e inmuebles, entre otros.					
Sensibles:	Registro de constitución física y lesiones (víctima u ofendido). Registro de arraigo del imputado en el cual se describe la media filiación del probable responsable. Información bancaria, de ser necesaria. Filiación política.					
Quién suministra	De manera directa del titular de los datos personales, y de manera indirecta por parte de terceros					
Cómo suministra	Documentos físicos y electrónicos.					
Finalidad:	Integración de Carpetas de Investigación por posibles actos constitutivos de delito.					
Tipo de Soporte	**Físico**	Sí	**Electrónico**	Sí	**Otro:**	No
	Descripción		Físico: Carpeta de Investigación con número identificativo. Electrónico: Bases de datos en hoja de cálculo. Reproducción de audiencias desahogadas con el Juez de Control y Juicio Oral, en disco compacto.			
	Características del lugar donde se resguardan		Archivero, computadora, dispositivos de almacenamiento.			
Participación en el ciclo de vida del dato personal	Obtención, conservación, utilización, transferencia y almacenamiento.					
VI.- Controles y Mecanismos de Seguridad de las transferencias **VII.- Resguardo de los Sistemas** **VIII.- Bitácoras para accesos y operación cotidiana** **XII.- Medidas de seguridad aplicadas a las instalaciones** **XIII.- Controles de identificación y autenticación de los usuarios**						
Nivel de seguridad	Básico		Medio	X	Alto	
Transferencias de datos personales						
Transferencia Electrónico y digital:	**Web service**	No	**Web Transfer**	No	**Nube**	No
	Discos externos	No	**Carpetas compartidas**	No	**CD**	No
	Correo	Sí	**USB**	No	**Otro:**	No
Medidas de seguridad transferencia electrónica digital	Correo oficial con protocolo de seguridad para transferencia electrónica (HTTPS)					
Transferencia Físico	Notificaciones a particulares, así como a diversas autoridades.					
Medidas de seguridad transferencia física	Notificaciones solo a las partes legitimadas, así como a sus autorizados o representantes, con acuse de recibo y previa identificación.					
Almacenamiento Sistemas de Datos Personales						
Almacenamiento Electrónico y digital:	**Servidor**	No	**Computadora**	Sí	**Nube**	Sí
	Discos externos	No	**Carpetas compartidas**	No	**CD**	Sí
	Correo	Sí	**USB**	Sí	**Otro:**	No

Medidas de seguridad almacenamiento electrónica digital	Usuario y contraseña para inicio de sesión en los equipos de cómputo; sistema de firewall; antivirus; así como bloqueo de pantalla por inactividad.					
Almacenamiento Físico	Expedientes físicos registrados con números consecutivos y acceso restringido					
Medidas de seguridad almacenamiento física	Archiveros, puerta de ingreso con llave, seguridad al ingreso de las instalaciones, y monitoreo por cámaras de seguridad en espacios que no cuentan con puerta y llave.					
Acceso a las instalaciones						
Seguridad perimetral exterior: Resguardo policial, cámaras de seguridad y puertas con llave.						
Seguridad perimetral interior: Puertas con llave, acceso restringido solo a personal autorizado y monitoreo permanente con cámaras de seguridad.						
Bitácoras para accesos y operación cotidiana						
Los datos que principalmente se registran en las bitácoras: Número de la Carpeta de Investigación; nombre de la víctima u ofendido, así como el probable responsable o en su caso la autoridad señalada como responsable; fecha de presentación de la denuncia; forma de recepción de la denuncia/querella; el delito por el cual se inició la investigación; etapa del proceso; lugar de los hechos; generales de la víctima u ofendido, así como del imputado, incluyendo el cargo y su adscripción; registro de actos de investigación; entre otros.						
Soporte de la bitácora:	**Físico**	X	**Electrónico**	X	**Otro:**	No
Lugar de almacenamiento:	Las Carpetas de Investigación en las Agencias del Ministerio Público, así como en la Comandancia de la Policía Investigadora, y el Libro de Gobierno en la Dirección de Control de Procesos y Audiencias.		**Tiempo**	Permanente (hasta en tanto se encuentren activas las Carpetas de Investigación).		
Como se asegura la integridad:	De manera física sólo se permite el acceso al personal autorizado para tal efecto. De manera electrónica sólo tiene acceso el resguardante del equipo de cómputo, previa autentificación.					
XI.- Gestión de Vulneraciones						
Datos que se registran: No se tiene						
Soporte del registro:	**Físico**		**Electrónico**		**Otro:**	
Lugar de almacenamiento:				**Tiempo**		
Como se asegura la integridad:						
XIV.- Respaldo y recuperación de datos						
Tipo de respaldo:	**Completo**	X	**Diferencial**		**Incremental**	
Medios para almacenar copias de seguridad	Documento electrónico					
XV.- Plan de Contingencia						
Se cuenta con Plan de contingencia			Si		No	X
Se realizan pruebas de eficiencia			Si		No	X
Se cuenta con un sitio redundante			Si		No	X
Tipo de sitio :	**Caliente**	No aplica	**Tibio**	No aplica	**Frío**	No aplica
	Propio	No aplica	**Subcontratado**	No aplica	**Tiempo**	No aplica
Procedimiento	No aplica					
Equipo	No aplica					
Personal	No aplica					
XVI.- Técnicas para la supresión y borrado seguro de los datos personales						
Datos del sistema que será cancelado: No aplica						
Denominación:	No aplica					
Motivos:	No aplica					
Plazos y condiciones para el bloqueo del sistema: No aplica						
Medidas de seguridad para el bloqueo y posterior supresión del sistema: No aplica						
Procedimiento para la supresión y período de conservación del sistema: No aplica						
Mecanismos para la supresión del sistema: No aplica						

Procesos de Compra

<table>
<tr><th colspan="6">Unidad Administrativa: Dirección de Administración, Planeación y Finanzas</th></tr>
<tr><td colspan="2">I.- Nombre del sistema:</td><td colspan="4">Procesos de compra.</td></tr>
<tr><td colspan="6">II.- Nombre cargo y adscripción del administrador del sistema
III.- funciones y obligaciones de las personas que traten datos personales.</td></tr>
<tr><td colspan="6">Administrador Responsable</td></tr>
<tr><td>Nombre:</td><td colspan="2">Norma Araceli Espinosa Limón</td><td>Cargo:</td><td colspan="2">Directora de Administración, Planeación y Finanzas</td></tr>
<tr><td colspan="6">Funciones:
Dirigir; supervisar y controlar la aplicación de políticas, controles, sistemas y procedimientos establecidos para la adecuada administración, y desarrollo de los Recursos Humanos, Financieros y Materiales de la FECC.
Dirigir, tramitar y supervisar la contratación de insumos, servicios generales, profesionales, técnicos o tecnológicos para el óptimo desempeño y funcionamiento de las distintas áreas de la FECC.
Instruir el cumplimiento y seguimiento del sistema de datos personales denominado Procesos de compras.
Establecer los mecanismos de control que aseguren la administración óptima y la adecuada operación del sistema de datos personales denominado Procesos de compras
Instruir el establecimiento de los parámetros y medidas de seguridad que debe contener el sistema de datos personales denominado Procesos de compras.</td></tr>
<tr><td colspan="6">Obligaciones:
Proteger los datos personales en posesión.
Tratar los de datos personales cuando sea exclusivamente en observancia a las facultades o atribuciones a la normatividad aplicable.
Vigilar y supervisar que se lleve a cabo el correcto resguardo de datos personales.</td></tr>
<tr><td colspan="6">Usuario Responsable 1</td></tr>
<tr><td colspan="2">Nombre:</td><td>Lorena Pérez Velasco</td><td>Cargo:</td><td colspan="2">Coordinadora Administrativa C</td></tr>
<tr><td colspan="6">Funciones:
Elaborar y dar seguimiento a los trámites viáticos para efectos de comisiones del personal de la FECC.
Llevar a cabo el control patrimonial mediante resguardos, de todos los bienes muebles e inmuebles bajo custodia de la FECC.
Apoyar en la realización de los proyectos que sean solicitados a través de la dirección.
Realizar el debido manejo de la información que integra el Sistema de Procesos de compras</td></tr>
<tr><td colspan="6">Obligaciones:
Proteger los datos personales en posesión.
Tratar los de datos personales cuando sea exclusivamente en observancia a las facultades o atribuciones a la normatividad aplicable.
Vigilar y supervisar que se lleve a cabo el correcto resguardo de datos personales.</td></tr>
<tr><td colspan="6">Encargado</td></tr>
<tr><td colspan="2">Nombre:</td><td>No aplica</td><td>Cargo:</td><td colspan="2">No aplica</td></tr>
<tr><td colspan="2">Funciones y Obligaciones:</td><td colspan="4">No aplica</td></tr>
<tr><td colspan="6">IV.- Inventario de datos personales
V.- Estructura y descripción de los sistemas</td></tr>
<tr><td>Ordinarios:</td><td colspan="5">Identificativos: Nombre, domicilio, teléfono particular, teléfono celular, correo electrónico, firma, RFC de proveedores.</td></tr>
<tr><td>Sensibles:</td><td colspan="5">No aplica</td></tr>
<tr><td colspan="2">Quién suministra</td><td colspan="4">De forma personal, directamente del titular e indirectamente del titular</td></tr>
<tr><td colspan="2">Cómo suministra</td><td colspan="4">Formato físico y electrónico.</td></tr>
<tr><td colspan="2">Finalidad:</td><td colspan="4">Sustanciar los procesos de compra, así como el pago a proveedores.</td></tr>
<tr><td rowspan="3">Tipo de Soporte</td><td>Físico</td><td>Sí</td><td>Electrónico</td><td>Sí</td><td>Otro: No</td></tr>
<tr><td>Descripción</td><td colspan="4">Físico: Expediente por partida de gasto. Electrónico: Base de datos en hoja de cálculo y cotizaciones.</td></tr>
<tr><td>Características del lugar donde se resguardan</td><td colspan="4">Archivero y Computadora</td></tr>
</table>

Participación en el ciclo de vida del dato personal	Obtención, conservación, utilización, transferencia y almacenamiento.					
VI.- Controles y Mecanismos de Seguridad de las transferencias **VII.- Resguardo de los Sistemas** **VIII.- Bitácoras para accesos y operación cotidiana** **XII.- Medidas de seguridad aplicadas a las instalaciones** **XIII.- Controles de identificación y autenticación de los usuarios**						
Nivel de seguridad	Básico	x	Medio		Alto	
Transferencias de datos personales						
Transferencia Electrónico y digital:	**Web service**	No aplica	**Web Transfer**	Sí	**Nube**	No aplica
	Discos externos	No aplica	**Carpetas compartidas**	No aplica	**CD**	No aplica
	Correo	Sí	**USB**	No aplica	**Otro:**	SIIF, SECG
Medidas de seguridad transferencia electrónica digital	Cifrado: Transferencias vía correo electrónico					
Transferencia Físico	Secretaría de Administración y Secretaría de la Hacienda Pública.					
Medidas de seguridad transferencia física	Personal autorizado y acuse de recibo					
Almacenamiento Sistemas de Datos Personales						
Almacenamiento Electrónico y digital:	**Servidor**	No aplica	**Computadora**	Sí	**Nube**	No aplica
	Discos externos	No aplica	**Carpetas compartidas**	No aplica	**CD**	No aplica
	Correo	Sí	**USB**	No aplica	**Otro:**	SIIF, SECG
Medidas de seguridad almacenamiento electrónica digital	Clave de acceso a sistemas, usuario, sistema de firewall, antivirus, contraseñas para acceder a las computadoras, sistemas de bloqueo de pantalla cada 5 minutos en las computadoras					
Almacenamiento Físico	Expedientes por partida presupuestal					
Medidas de seguridad almacenamiento física	Archiveros y puertas con chapa para accesar a la Dirección de Administración, Planeación y Finanzas.					
Acceso a las instalaciones						
Seguridad perimetral exterior: Resguardo policial, cámaras de seguridad y puerta con llave						
Seguridad perimetral interior: Puerta con llave						
Bitácoras para accesos y operación cotidiana						
Los datos que se registran en las bitácoras: Número de Expediente, fecha de ingreso, nombre del proveedor, firma, número de contrato, número de solicitud del sistema.						
Soporte de la bitácora:	**Físico**	x	**Electrónico**	x	**Otro:**	
Lugar de almacenamiento:	Física: Área común de la Dirección de Administración, Planeación y Finanzas, archivero. Electrónica: Computadora, base de datos en hoja de cálculo.			**Tiempo**	10 años	
Como se asegura la integridad:	Físico: Acceso a personal autorizado. Electrónico: Acceso solo al resguardante de computadora con contraseña.					
XI.- Gestión de Vulneraciones						
Datos que se registran: No se tiene						
Soporte del registro:	**Físico**		**Electrónico**		**Otro:**	
Lugar de almacenamiento:				**Tiempo**		
Como se asegura la integridad:						
XIV.- Respaldo y recuperación de datos						
Tipo de respaldo:	**Completo**	x	**Diferencial**		**Incremental**	
Medios para almacenar copias de seguridad	Documento electrónico					
XV.- Plan de Contingencia						
Se cuenta con Plan de contingencia			Si		No	x
Se realizan pruebas de eficiencia			Si		No	x

Se cuenta con un sitio redundante			Si		No	x
Tipo de sitio :	**Caliente**	No aplica	**Tibio**	No aplica	**Frío**	No aplica
	Propio	No aplica	**Subcontratado**	No aplica	**Tiempo**	No aplica
Procedimiento	No aplica					
Equipo	No aplica					
Personal	No aplica					
XVI.- Técnicas para la supresión y borrado seguro de los datos personales						
Datos del sistema que será cancelado: No aplica						
Denominación:	No aplica					
Motivos:	No aplica					
Plazos y condiciones para el bloqueo del sistema: No aplica						
Medidas de seguridad para el bloqueo y posterior supresión del sistema: No aplica						
Procedimiento para la supresión y período de conservación del sistema: No aplica						
Mecanismos para la supresión del sistema: No aplica						

Contratación de Personal

<table>
<tr><th colspan="4">Unidad Administrativa: Coordinación de la Unidad de Transparencia e Información</th></tr>
<tr><td colspan="2">I.- Nombre del sistema:</td><td colspan="2">Contratación de Personal</td></tr>
<tr><td colspan="4">II.- Nombre cargo y adscripción del administrador del sistema
III.- funciones y obligaciones de las personas que traten datos personales.</td></tr>
<tr><td colspan="4">Administrador Responsable</td></tr>
<tr><td>Nombre:</td><td>Norma Araceli Espinosa Limón</td><td>Cargo:</td><td>Directora de Administración, Planeación y Finanzas</td></tr>
<tr><td colspan="4">Funciones y Obligaciones:
Dirigir; supervisar y controlar la aplicación de políticas, controles, sistemas y procedimientos establecidos para la adecuada administración, y desarrollo de los Recursos, Humanos, Financieros y Materiales de la FECC.
Implementar y desarrollar los programas de capacitación, desarrollo de personal y el Servicio Profesional de Carrera de los servicios públicos y elementos operativos.
Coordinar y contratar, en conjunto con la Secretaria de Administración la capacitación institucional y especializada del personal, coadyuvando en la profesionalización, mejora y desarrollo de los servicios públicos de la FECC, sus Órganos e Instancias Administrativas.
Informar tanto a los organismos públicos como privados que así lo soliciten los antecedentes laborales del personal activo e inactivo de la FECC.
Proponer al interior de la dependencia criterios de evaluación y seguimiento acordes con el modelo de planeación establecido en el Poder Ejecutivo del Estado.</td></tr>
<tr><td colspan="4">Obligaciones:
Proteger los datos personales en posesión.
Tratar los de datos personales cuando sea exclusivamente en observancia a las facultades o atribuciones a la normatividad aplicable.
Vigilar y supervisar que se lleve a cabo el correcto resguardo de datos personales.</td></tr>
<tr><td colspan="4">Usuario Responsable 1</td></tr>
<tr><td>Nombre:</td><td>María Antonieta González Pérez</td><td>Cargo:</td><td>Auxiliar Administrativo</td></tr>
<tr><td colspan="4">Funciones y Obligaciones:
Registrar en bases de datos la documentación que ingrese y egrese del área.
Recibir, clasificar y distribuir a las áreas respectivas la documentación ingresada.
Archivar y tramitar la documentación ingresada.
Mantener actualizados los archivos y sistemas operativos del área.
Realizar el debido manejo de la información que integra el Sistema de Contratación de personal.</td></tr>
<tr><td colspan="4">Obligaciones:
Proteger los datos personales en posesión.
Tratar los de datos personales cuando sea exclusivamente en observancia a las facultades o atribuciones que la normatividad aplicable.
Vigilar y supervisar que se lleve a cabo el correcto resguardo de datos personales.</td></tr>
<tr><td colspan="4">Encargado</td></tr>
<tr><td>Nombre:</td><td>No aplica</td><td>Cargo:</td><td>No aplica</td></tr>
<tr><td colspan="4">Funciones y Obligaciones:</td></tr>
<tr><td colspan="4">IV.- Inventario de datos personales
V.- Estructura y descripción de los sistemas</td></tr>
<tr><td>Ordinarios:</td><td colspan="3">Identificativos: Nombre, acta de nacimiento actualizada, fecha de nacimiento, nacionalidad, cartilla del servicio militar nacional liberada, título de licenciatura, carta de no antecedentes penales, currículum vitae actualizado y firmado, número de teléfono, estado civil; nivel académico, experiencia laboral, referencias personales/laborales, constancia de no sanción administrativa expedida por la Contraloría del Estado, credencial de elector con fotografía IFE/INE, licencia de conducir, comprobante de ingresos, número de seguro social, comprobante de domicilio, CURP, RFC con homoclave, fotografía, cuenta personal de correo electrónico, nombramientos de personal.</td></tr>
<tr><td>Sensibles:</td><td colspan="3">Salud: Resultados de evaluaciones médicas y psicológicas, certificados de médicos y de no ingravidez en su caso, tipo de sangre.</td></tr>
<tr><td colspan="2">Quién suministra</td><td colspan="2">De forma personal y directamente del titular</td></tr>
<tr><td colspan="2">Cómo suministra</td><td colspan="2">Formato físico</td></tr>
</table>

Finalidad:	Iniciar con el proceso de reclutamiento y selección de personal para algún puesto operativo o administrativo para la contratación de personal y la creación del expediente laboral					
Tipo de Soporte	**Físico**	Sí	**Electrónico**	Sí	**Otro:**	No
	Descripción		Físico: Expediente ordenados por adscripción y en orden alfabético. Electrónico: Carpetas ordenadas por nombre del servidor público, y base de datos en hoja de cálculo.			
	Características del lugar donde se resguardan		Archivero y Computadora			
Participación en el ciclo de vida del dato personal	Obtención, conservación, utilización, transferencia y almacenamiento.					
VI.- Controles y Mecanismos de Seguridad de las transferencias **VII.- Resguardo de los Sistemas** **VIII.- Bitácoras para accesos y operación cotidiana** **XII.- Medidas de seguridad aplicadas a las instalaciones** **XIII.- Controles de identificación y autenticación de los usuarios**						
Nivel de seguridad	Básico		Medio		Alto	x
Transferencias de datos personales						
Transferencia Electrónico y digital:	**Web service**	No aplica	**Web Transfer**	no aplica	**Nube**	Si
	Discos externos	No aplica	**Carpetas compartidas**	No aplica	**CD**	No aplica
	Correo	Sí	**USB**	No aplica	**Otro:**	SIAN
Medidas de seguridad transferencia electrónica digital	Cifrado https. SIAN					
Transferencia Físico	Secretaría de Administración y Fiscalía del Estado.					
Medidas de seguridad transferencia física	Personal autorizado y acuse de recibo					
Almacenamiento Sistemas de Datos Personales						
Almacenamiento Electrónico y digital:	**Servidor**	No aplica	**Computadora**	Sí	**Nube**	SÍ
	Discos externos	No aplica	**Carpetas compartidas**	No aplica	**CD**	No aplica
	Correo	Sí	**USB**	Sí	**Otro:**	SIAN
Medidas de seguridad almacenamiento electrónica digital	Clave de acceso a sistemas, usuario, sistema de firewall, antivirus, contraseñas para acceder a las computadoras, sistemas de bloqueo de pantalla cada 5 minutos en las computadoras					
Almacenamiento Físico	Expediente ordenado por adscripción y en orden alfabético.					
Medidas de seguridad almacenamiento física	Archiveros con llave en el área de la Dirección de Administración, Planeación y Finanzas.					
Acceso a las instalaciones						
Seguridad perimetral exterior: Resguardo policial, cámaras de seguridad y puerta con llave						
Seguridad perimetral interior: Puerta con llave y cámaras de seguridad.						
Bitácoras para accesos y operación cotidiana						
Los datos que se registran en las bitácoras: No aplica						
Soporte de la bitácora:	**Físico**		**Electrónico**		**Otro:**	
Lugar de almacenamiento:				**Tiempo**	Permanente	
Como se asegura la integridad:						
XI.- Gestión de Vulneraciones						
Datos que se registran: No se tiene						
Soporte del registro:	**Físico**		**Electrónico**		**Otro:**	
Lugar de almacenamiento:				**Tiempo**		
Como se asegura la integridad:						
XIV.- Respaldo y recuperación de datos						
Tipo de respaldo:	**Completo**	x	**Diferencial**		**Incremental**	

Medios para almacenar copias de seguridad	Documento electrónico					
XV.- Plan de Contingencia						
Se cuenta con Plan de contingencia			Si		No	x
Se realizan pruebas de eficiencia			Si		No	x
Se cuenta con un sitio redundante			Si		No	x
Tipo de sitio :	**Caliente**	No aplica	**Tibio**	No aplica	**Frío**	No aplica
	Propio	No aplica	**Subcontratado**	No aplica	**Tiempo**	No aplica
Procedimiento	No aplica					
Equipo	No aplica					
Personal	No aplica					
XVI.- Técnicas para la supresión y borrado seguro de los datos personales						
Datos del sistema que será cancelado: No aplica						
Denominación:	No aplica					
Motivos:	No aplica					
Plazos y condiciones para el bloqueo del sistema: No aplica						
Medidas de seguridad para el bloqueo y posterior supresión del sistema: No aplica						
Procedimiento para la supresión y período de conservación del sistema: No aplica						
Mecanismos para la supresión del sistema: No aplica						

*****NOTA: El Sistema Integral de Administración de Nomina (SIAN), no es administrado por este Sujeto Obligado.

Solicitudes de Acceso a Información Pública

<table>
<tr><th colspan="4">Unidad Administrativa: Coordinación de la Unidad de Transparencia e Información</th></tr>
<tr><td colspan="2">I.- Nombre del sistema:</td><td colspan="2">Solicitudes de Acceso a Información Pública</td></tr>
<tr><td colspan="4">II.- Nombre cargo y adscripción del administrador del sistema
III.- funciones y obligaciones de las personas que traten datos personales.</td></tr>
<tr><td colspan="4">Administrador Responsable</td></tr>
<tr><td>Nombre:</td><td>Beatriz Adriana Hernández Portillo</td><td>Cargo:</td><td>Coordinadora de la Unidad de Transparencia e Información</td></tr>
<tr><td colspan="4">Funciones:
Coordinar y dirigir la recepción y trámite a las solicitudes de acceso a la información recibidas de forma personal o a través del Sistema Infomex.
Supervisar la canalización de las peticiones de la información solicitada a las áreas correspondientes y dar respuesta en tiempo y forma a las solicitudes de información.
Diseñar, proponer e implementar programas de acción y asistencia a los particulares en la elaboración de solicitudes de acceso a la información.
Implementar y vigilar los mecanismos de registro y control de solicitudes de acceso a la información.
Convocar y remitir al Comité de Transparencia la Información que requiera ser clasificada y dar seguimiento a los acuerdos o criterios emitidos en sesiones ordinarias y extraordinarias.
Las demás que le atribuyen la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios, su reglamento y la Ley de Protección de datos personales en posesión de los sujetos obligados.
Instruir el cumplimiento y seguimiento del sistema de datos personales denominado Solicitudes de Acceso a Información Pública.
Establecer los mecanismos de control que aseguren la administración óptima y la adecuada operación del Sistema de Solicitudes de Acceso a Información Pública.
Instruir el establecimiento de los parámetros y medidas de seguridad que debe contener el catálogo.</td></tr>
<tr><td colspan="4">Obligaciones:
Proteger los datos personales en posesión.
Tratar los de datos personales cuando sea exclusivamente en observancia a las facultades o atribuciones a la normatividad aplicable.
Vigilar y supervisar que se lleve a cabo el correcto resguardo de datos personales.</td></tr>
<tr><td colspan="4">Usuario Responsable 1</td></tr>
<tr><td>Nombre:</td><td>Margarita Ramírez Esparza</td><td>Cargo:</td><td>Analista Digitalizador de Transparencia</td></tr>
<tr><td colspan="4">Funciones:
Recibir y dar trámite a las solicitudes de acceso a la información realizando los trámites internos necesarios para obtener la información solicitada y así estar en posibilidades de otorgar una respuesta en tiempo y forma al solicitante.
Asistir a los particulares en la elaboración de solicitudes, y en su caso, orientarlos sobre los sujetos obligados que pudieran tener la información que solicitan.
Realizar un control de registro de solicitudes de acceso a la información, sus resultados y costos.
Remitir al Comité de Transparencia de esta Institución la información que por su naturaleza requiera ser clasificada y llevar a cabo el registro de acuerdos o criterios emitidos por dicho Comité.
Apoyar en la promoción de la cultura de la transparencia y el acceso a la información pública al interior de la FECC.
Realizar el debido manejo de la información que integra el Sistema de Solicitudes de Acceso a la Información</td></tr>
<tr><td colspan="4">Obligaciones:
Proteger los datos personales en posesión.
Tratar los de datos personales cuando sea exclusivamente en observancia a las facultades o atribuciones a la normatividad aplicable.
Vigilar y supervisar que se lleve a cabo el correcto resguardo de datos personales.</td></tr>
<tr><td colspan="4">Encargado</td></tr>
<tr><td>Nombre:</td><td>No aplica</td><td>Cargo:</td><td>no aplica</td></tr>
<tr><td colspan="2">Funciones y Obligaciones:</td><td colspan="2">No aplica</td></tr>
<tr><td colspan="4">IV.- Inventario de datos personales
V.- Estructura y descripción de los sistemas</td></tr>
<tr><td>Ordinarios:</td><td colspan="3">Identificativos: nombre, domicilio, teléfono particular, teléfono celular, correo electrónico, firma, nacionalidad, rango edad, escolaridad y ocupación.</td></tr>
</table>

Sensibles:	No aplica					
Quién suministra	De forma personal, directamente del titular e indirectamente del titular					
Cómo suministra	Formato físico, formularios electrónicos, correo electrónico					
Finalidad:	Dar respuesta a las solicitudes de acceso a la información pública					
Tipo de Soporte	**Físico**	Sí	**Electrónico**	Sí	**Otro:**	No
	Descripción		Físico: Expediente numerado de la solicitud. Electrónico: Base de datos en hoja de cálculo.			
	Características del lugar donde se resguardan		Archivero y Computadora			
Participación en el ciclo de vida del dato personal	Obtención, conservación, utilización, transferencia y almacenamiento.					
VI.- Controles y Mecanismos de Seguridad de las transferencias **VII.- Resguardo de los Sistemas** **VIII.- Bitácoras para accesos y operación cotidiana** **XII.- Medidas de seguridad aplicadas a las instalaciones** **XIII.- Controles de identificación y autenticación de los usuarios**						
Nivel de seguridad	Básico	x	Medio		Alto	
Transferencias de datos personales						
Transferencia Electrónico y digital:	**Web service**	No aplica	**Web Transfer**	Sí	**Nube**	No aplica
	Discos externos	No aplica	**Carpetas compartidas**	No aplica	**CD**	No aplica
	Correo	Sí	**USB**	No aplica	**Otro:**	Infomex, PNT
Medidas de seguridad transferencia electrónica digital	Correo oficial, Plataforma Nacional de Transparencia y sistema Infomex Jalisco; todos con protocolo de seguridad para transferencia electrónica (HTTPS).					
Transferencia Físico	Notificaciones a Sujetos Obligados e ITEI					
Medidas de seguridad transferencia física	Personal autorizado y acuse de recibo					
Almacenamiento Sistemas de Datos Personales						
Almacenamiento Electrónico y digital:	**Servidor**	No aplica	**Computadora**	Sí	**Nube**	No aplica
	Discos externos	No aplica	**Carpetas compartidas**	No aplica	**CD**	No aplica
	Correo	Sí	**USB**	Sí	**Otro:**	Infomex, PNT
Medidas de seguridad almacenamiento electrónica digital	Clave de acceso a sistemas, usuario, clave de acceso a la plataforma nacional y sistema Infomex, sistema de firewall, antivirus, contraseñas para acceder a las computadoras, sistemas de bloqueo de pantalla cada 5 minutos en las computadoras					
Almacenamiento Físico	Expedientes consecutivos					
Medidas de seguridad almacenamiento física	Archiveros y puertas con chapa para accesar a la Unidad de Transparencia					
Acceso a las instalaciones						
Seguridad perimetral exterior: Resguardo policial, cámaras de seguridad y puerta con llave						
Seguridad perimetral interior: Puerta con llave						
Bitácoras para accesos y operación cotidiana						
Los datos que se registran en las bitácoras: Número de Expediente, Fecha de ingreso, Nombre del solicitante, Solicitud, Medio de presentación, Folio, Fecha de término, Fecha de Respuesta, Nombre de quien responde.						
Soporte de la bitácora:	**Físico**	x	**Electrónico**	x	**Otro:**	
Lugar de almacenamiento:	Física: Unidad de Transparencia, Archivero. Electrónica: Computadora Base de datos en hoja de cálculo.			**Tiempo**	3 años	
Como se asegura la integridad:	Físico: Acceso a personal autorizado. Electrónico: Acceso solo al resguardante de computadora con contraseña					
XI.- Gestión de Vulneraciones						
Datos que se registran: No se tiene						

Soporte del registro:	**Físico**	No aplica	**Electrónico**	No aplica	**Otro:**	No aplica
Lugar de almacenamiento:	No aplica			**Tiempo**	No aplica	
Como se asegura la integridad:	No aplica					
XIV.- Respaldo y recuperación de datos						
Tipo de respaldo:	**Completo**	x	**Diferencial**		**Incremental**	
Medios para almacenar copias de seguridad	Documento electrónico					
XV.- Plan de Contingencia						
Se cuenta con Plan de contingencia			Si		No	x
Se realizan pruebas de eficiencia			Si		No	x
Se cuenta con un sitio redundante			Si		No	x
Tipo de sitio :	**Caliente**	No aplica	**Tibio**	No aplica	**Frío**	No aplica
	Propio	No aplica	**Subcontratado**	No aplica	**Tiempo**	No aplica
Procedimiento	No aplica					
Equipo	No aplica					
Personal	No aplica					
XVI.- Técnicas para la supresión y borrado seguro de los datos personales						
Datos del sistema que será cancelado: No aplica						
Denominación:	No aplica					
Motivos:	No aplica					
Plazos y condiciones para el bloqueo del sistema: No aplica						
Medidas de seguridad para el bloqueo y posterior supresión del sistema: No aplica						
Procedimiento para la supresión y período de conservación del sistema: No aplica						

*****NOTA: El Sistema INFOMEX y la Plataforma Nacional de Transparencia (PNT), no son administradas por este Sujeto Obligado.

Solicitudes de Ejercicio de Derechos ARCO

<table>
<tr><th colspan="4">Unidad Administrativa: Coordinación de la Unidad de Transparencia e Información</th></tr>
<tr><td colspan="2">I.- Nombre del sistema:</td><td colspan="2">Solicitudes de Ejercicio de Derechos ARCO</td></tr>
<tr><td colspan="4">II.- Nombre cargo y adscripción del administrador del sistema
III.- funciones y obligaciones de las personas que traten datos personales.</td></tr>
<tr><td colspan="4">Administrador Responsable</td></tr>
<tr><td>Nombre:</td><td>Beatriz Adriana Hernández Portillo</td><td>Cargo:</td><td>Coordinadora de la Unidad de Transparencia e Información</td></tr>
<tr><td colspan="4">Funciones:
Diseñar e implementar el cumplimiento de las medidas, controles y acciones para la protección de datos personales en la Dependencia.
Proponer y establecer al Comité de Transparencia los mecanismos correspondientes en los procedimientos internos que aseguren y fortalezcan con mayor eficiencia la gestión de solicitudes para el ejercicio de los derechos ARCO.
Las demás que le atribuyen la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios, su reglamento y la Ley de Protección de datos personales en posesión de los sujetos obligados.
Instruir el cumplimiento y seguimiento del sistema de datos personales denominado Solicitudes de Ejercicio de Derechos ARCO.
Establecer los mecanismos de control que aseguren la administración óptima y la adecuada operación del Sistema de Solicitudes de Ejercicio de Derechos ARCO.
Instruir el establecimiento de los parámetros y medidas de seguridad que debe contener el catálogo.</td></tr>
<tr><td colspan="4">Obligaciones:
Proteger los datos personales en posesión.
Tratar los de datos personales cuando sea exclusivamente en observancia a las facultades o atribuciones a la normatividad aplicable.
Vigilar y supervisar que se lleve a cabo el correcto resguardo de datos personales.
Realizar el debido manejo de la información que integra el Sistema de Solicitudes de Ejercicio de Derechos ARCO.</td></tr>
<tr><td colspan="4">Usuario Responsable 1</td></tr>
<tr><td>Nombre:</td><td>Margarita Ramírez Esparza</td><td>Cargo:</td><td>Analista Digitalizador de Transparencia</td></tr>
<tr><td colspan="4">Funciones:
Auxiliar al Titular de la Unidad de Transparencia para asesorar al Fiscal Especializado y a los Titulares de las Unidades Administrativas con relación al ejercicio del derecho a la protección de datos personales.
Coadyuvar en la realización de procedimientos internos y la elaboración de respuestas de solicitudes para el ejercicio de los derechos ARCO a fin de dar cumplimiento a lo estipulado y normatividad aplicable vigente en la materia.
Diseñar e implementar en coordinación con las área o unidades administrativas competentes, el cumplimento de las medidas, controles y acciones para la protección de datos personales. Así como proponer mecanismos para asegurar que los datos personales solo se entreguen a su titular o sus representantes debidamente acreditados.
Las demás que le atribuyan la Ley de Transparencia y acceso a la información Pública del Estado de Jalisco y sus Municipios, su reglamento y la Ley de protección de datos personales en posesión de sujetos obligados.</td></tr>
<tr><td colspan="4">Obligaciones:
Proteger los datos personales en posesión.
Tratar los de datos personales cuando sea exclusivamente en observancia a las facultades o atribuciones a la normatividad aplicable.
Vigilar y supervisar que se lleve a cabo el correcto resguardo de datos personales.</td></tr>
<tr><td colspan="4">Encargado</td></tr>
<tr><td>Nombre:</td><td>No aplica</td><td>Cargo:</td><td>No aplica</td></tr>
<tr><td colspan="4">Funciones y Obligaciones: No aplica</td></tr>
<tr><td colspan="4">IV.- Inventario de datos personales
V.- Estructura y descripción de los sistemas</td></tr>
<tr><td>Ordinarios:</td><td colspan="3">Identificativos: nombre, domicilio, teléfono particular, teléfono celular, firma, nacionalidad, rango edad, escolaridad y ocupación.</td></tr>
</table>

Sensibles:	No aplica					
Quién suministra	De forma personal, directamente del titular e indirectamente del titular					
Cómo suministra	Formato físico, formularios electrónicos, correo electrónico					
Finalidad:	Dar respuesta a las solicitudes de ejercicio de Derecho de acceso, rectificación y cancelación de datos personales, así como de oposición y/o cese al tratamiento de los mismos presentadas ante el responsable.					
Tipo de Soporte	**Físico**	Sí	**Electrónico**	Sí	**Otro:**	No
	Descripción		Físico: Expediente numerado de la solicitud. Electrónico: Base de datos en hoja de cálculo.			
	Características del lugar donde se resguardan		Archivero y Computadora			
Participación en el ciclo de vida del dato personal	Obtención, conservación, utilización, transferencia y almacenamiento.					
VI.- Controles y Mecanismos de Seguridad de las transferencias **VII.- Resguardo de los Sistemas** **VIII.- Bitácoras para accesos y operación cotidiana** **XII.- Medidas de seguridad aplicadas a las instalaciones** **XIII.- Controles de identificación y autenticación de los usuarios**						
Nivel de seguridad	Básico	x	Medio	x	Alto	x
Transferencias de datos personales						
Transferencia Electrónico y digital:	**Web service**	No aplica	**Web Transfer**	Sí	**Nube**	No aplica
	Discos externos	No aplica	**Carpetas compartidas**	No aplica	**CD**	No aplica
	Correo	Sí	**USB**	No aplica	**Otro:**	Infomex, PNT
Medidas de seguridad transferencia electrónica digital	cifrado https. En plataforma nacional de transparencia y sistema Infomex					
Transferencia Físico	Notificaciones a Sujetos Obligados e ITEI					
Medidas de seguridad transferencia física	Personal autorizado y acuse de recibo					
Almacenamiento Sistemas de Datos Personales						
Almacenamiento Electrónico y digital:	**Servidor**	No aplica	**Computadora**	Sí	**Nube**	No aplica
	Discos externos	No aplica	**Carpetas compartidas**	No aplica	**CD**	No aplica
	Correo	Sí	**USB**	Sí	**Otro:**	Infomex, PNT
Medidas de seguridad almacenamiento electrónica digital	Clave de acceso a sistemas, usuario, clave de acceso a la plataforma nacional y sistema Infomex, sistema de firewall, antivirus, contraseñas para acceder a las computadoras, sistemas de bloqueo de pantalla cada 5 minutos en las computadoras					
Almacenamiento Físico	Expedientes consecutivos					
Medidas de seguridad almacenamiento física	Archiveros y puertas con chapa para accesar a la Unidad de Transparencia					
Acceso a las instalaciones						
Seguridad perimetral exterior: Resguardo policial, cámaras de seguridad y puerta con llave						
Seguridad perimetral interior: Puerta con llave						
Bitácoras para accesos y operación cotidiana						
Los datos que se registran en las bitácoras: Número de Expediente, Fecha de ingreso, Nombre del solicitante, Solicitud, Medio de presentación, Folio, Fecha de término, Fecha de Respuesta, Nombre de quien responde.						
Soporte de la bitácora:	**Físico**	x	**Electrónico**	x	**Otro:**	
Lugar de almacenamiento:	Física: Unidad de Transparencia, Archivero. Electrónica: Computadora Base de datos en hoja de cálculo.		**Tiempo**	3 años		
Como se asegura la integridad:	Físico: Acceso a personal autorizado. Electrónico: Acceso solo al resguardante de computadora con contraseña					

XI.- Gestión de Vulneraciones						
Datos que se registran: No se tiene						
Soporte del registro:	**Físico**	No aplica	**Electrónico**	No aplica	**Otro:**	No aplica
Lugar de almacenamiento:	No aplica			**Tiempo**	No aplica	
Como se asegura la integridad:	No aplica					
XIV.- Respaldo y recuperación de datos						
Tipo de respaldo:	**Completo**	x	**Diferencial**		**Incremental**	
Medios para almacenar copias de seguridad	Documento electrónico					
XV.- Plan de Contingencia						
Se cuenta con Plan de contingencia			Si		No	x
Se realizan pruebas de eficiencia			Si		No	x
Se cuenta con un sitio redundante			Si		No	x
Tipo de sitio :	**Caliente**	No aplica	**Tibio**	No aplica	**Frío**	No aplica
	Propio	No aplica	**Subcontratado**	No aplica	**Tiempo**	No aplica
Procedimiento	No aplica					
Equipo	No aplica					
Personal	No aplica					
XVI.- Técnicas para la supresión y borrado seguro de los datos personales						
Datos del sistema que será cancelado: No aplica						
Denominación:	No aplica					
Motivos:	No aplica					
Plazos y condiciones para el bloqueo del sistema: No aplica						
Medidas de seguridad para el bloqueo y posterior supresión del sistema: No aplica						
Procedimiento para la supresión y período de conservación del sistema: No aplica						
Mecanismos para la supresión del sistema: No aplica						

*****NOTA: El Sistema INFOMEX y la Plataforma Nacional de Transparencia (PNT), no son administradas por este Sujeto Obligado.

Recursos de Transparencia

<table>
<tr><th colspan="6">Unidad Administrativa: Coordinación de la Unidad de Transparencia e Información</th></tr>
<tr><td colspan="2">I.- Nombre del sistema:</td><td colspan="4">Recursos de Transparencia</td></tr>
<tr><td colspan="6">II.- Nombre cargo y adscripción del administrador del sistema
III.- funciones y obligaciones de las personas que traten datos personales.</td></tr>
<tr><td colspan="6">Administrador Responsable</td></tr>
<tr><td>Nombre:</td><td colspan="2">Beatriz Adriana Hernández Portillo</td><td>Cargo:</td><td colspan="2">Coordinadora de la Unidad de Transparencia e Información</td></tr>
<tr><td colspan="6">Funciones:
Vigilar que la información pública de carácter fundamental que genera la FECC, como sujeto obligado sea solicitada, recabada, actualizada, publicada periódica y permanentemente por medios electrónicos, tal como lo marca la legislación vigente.
Las demás que le atribuyen la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios, su reglamento y la Ley de Protección de datos personales en posesión de los sujetos obligados.
Instruir el cumplimiento y seguimiento del sistema de datos personales denominado Recursos de Transparencia.
Establecer los mecanismos de control que aseguren la administración óptima y la adecuada operación del Sistema de Recursos de Transparencia.
Instruir el establecimiento de los parámetros y medidas de seguridad que debe contener el catálogo.</td></tr>
<tr><td colspan="6">Obligaciones:
Proteger los datos personales en posesión.
Tratar los de datos personales cuando sea exclusivamente en observancia a las facultades o atribuciones a la normatividad aplicable.
Vigilar y supervisar que se lleve a cabo el correcto resguardo de datos personales.</td></tr>
<tr><td colspan="6">Usuario Responsable 1</td></tr>
<tr><td colspan="2">Nombre:</td><td>Margarita Ramírez Esparza</td><td>Cargo:</td><td colspan="2">Analista Digitalizador de Transparencia</td></tr>
<tr><td colspan="6">Funciones:
Recabar, actualizar y publicar periódicamente y permanentemente, por medios electrónicos la información pública de carácter fundamental que deba generar el Despacho del Fiscal Especial en Combate a la Corrupción y sus Unidades Administrativas como sujeto obligado.
Las demás que le atribuyan la Ley de Transparencia y acceso a la información Pública del Estado de Jalisco y sus Municipios, su reglamento y la Ley de protección de datos personales en posesión de sujetos obligados.
Realizar el debido manejo de la información que integra el Sistema de Recursos de Transparencia</td></tr>
<tr><td colspan="6">Obligaciones:
Proteger los datos personales en posesión.
Tratar los de datos personales cuando sea exclusivamente en observancia a las facultades o atribuciones a la normatividad aplicable.
Vigilar y supervisar que se lleve a cabo el correcto resguardo de datos personales.</td></tr>
<tr><td colspan="6">Encargado</td></tr>
<tr><td colspan="2">Nombre:</td><td>No aplica</td><td>Cargo:</td><td colspan="2">No aplica</td></tr>
<tr><td colspan="6">Funciones y Obligaciones: No aplica</td></tr>
<tr><td colspan="6">IV.- Inventario de datos personales
V.- Estructura y descripción de los sistemas</td></tr>
<tr><td>Ordinarios:</td><td colspan="5">Identificativos: nombre, domicilio, teléfono particular, teléfono celular, firma, nacionalidad, rango edad, escolaridad y ocupación.</td></tr>
<tr><td>Sensibles:</td><td colspan="5">No aplica</td></tr>
<tr><td colspan="2">Quién suministra</td><td colspan="4">De forma personal, directamente del titular e indirectamente del titular</td></tr>
<tr><td colspan="2">Cómo suministra</td><td colspan="4">Formato físico, formularios electrónicos, correo electrónico</td></tr>
<tr><td colspan="2">Finalidad:</td><td colspan="4">Dar respuesta a las solicitudes de acceso a la información pública</td></tr>
<tr><td colspan="2" rowspan="2">Tipo de Soporte</td><td>Físico</td><td>Sí</td><td>Electrónico</td><td>Sí</td><td>Otro:</td><td>No</td></tr>
<tr><td>Descripción</td><td colspan="5">Físico: Expediente numerado de la solicitud.
Electrónico: Base de datos en hoja de cálculo.</td></tr>
</table>

	Características del lugar donde se resguardan	Archivero y Computadora				
Participación en el ciclo de vida del dato personal	Obtención, conservación, utilización, transferencia y almacenamiento.					
VI.- Controles y Mecanismos de Seguridad de las transferencias **VII.- Resguardo de los Sistemas** **VIII.- Bitácoras para accesos y operación cotidiana** **XII.- Medidas de seguridad aplicadas a las instalaciones** **XIII.- Controles de identificación y autenticación de los usuarios**						
Nivel de seguridad	Básico	x	Medio	x	Alto	x
Transferencias de datos personales						
Transferencia Electrónico y digital:	**Web service**	No aplica	**Web Transfer**	Sí	**Nube**	No aplica
	Discos externos	No aplica	**Carpetas compartidas**	No aplica	**CD**	No aplica
	Correo	Sí	**USB**	No aplica	**Otro:**	Infomex, PNT
Medidas de seguridad transferencia electrónica digital	cifrado https. En plataforma nacional de transparencia y sistema Infomex					
Transferencia Físico	Notificaciones al ITEI					
Medidas de seguridad transferencia física	Personal autorizado y acuse de recibo					
Almacenamiento Sistemas de Datos Personales						
Almacenamiento Electrónico y digital:	**Servidor**	No aplica	**Computadora**	Sí	**Nube**	No aplica
	Discos externos	No aplica	**Carpetas compartidas**	No aplica	**CD**	No aplica
	Correo	Sí	**USB**	Sí	**Otro:**	Infomex, PNT
Medidas de seguridad almacenamiento electrónica digital	Clave de acceso a sistemas, usuario, clave de acceso a la plataforma nacional y sistema Infomex, sistema de firewall, antivirus, contraseñas para acceder a las computadoras, sistemas de bloqueo de pantalla cada 5 minutos en las computadoras					
Almacenamiento Físico	Expedientes consecutivos					
Medidas de seguridad almacenamiento física	Archiveros y puertas con chapa para accesar a la Unidad de Transparencia.					
Acceso a las instalaciones						
Seguridad perimetral exterior: Resguardo policial, cámaras de seguridad y puerta con llave						
Seguridad perimetral interior: Puerta con llave						
Bitácoras para accesos y operación cotidiana						
Los datos que se registran en las bitácoras: Número de Expediente, Fecha de ingreso, Nombre del recurrente, Solicitud, Medio de presentación, Folio, Fecha de término, Fecha de Respuesta, Nombre de quien responde.						
Soporte de la bitácora:	**Físico**	x	**Electrónico**	x	**Otro:**	
Lugar de almacenamiento:	Física: Unidad de Transparencia, Archivero. Electrónica: Computadora Base de datos en hoja de cálculo.		**Tiempo**	3 años		
Como se asegura la integridad:	Físico: Acceso a personal autorizado. Electrónico: Acceso solo al resguardante de computadora con contraseña					
XI.- Gestión de Vulneraciones						
Datos que se registran: No se tiene						
Soporte del registro:	**Físico**	No aplica	**Electrónico**	No aplica	**Otro:**	No aplica
Lugar de almacenamiento:	No aplica		**Tiempo**	No aplica		
Como se asegura la integridad:	No aplica					
XIV.- Respaldo y recuperación de datos						
Tipo de respaldo:	**Completo**	x	**Diferencial**		**Incremental**	

Medios para almacenar copias de seguridad		Documento electrónico				
XV.- Plan de Contingencia						
Se cuenta con Plan de contingencia			Si		No	x
Se realizan pruebas de eficiencia			Si		No	x
Se cuenta con un sitio redundante			Si		No	x
Tipo de sitio :	**Caliente**	No aplica	**Tibio**	No aplica	**Frío**	No aplica
	Propio	No aplica	**Subcontratado**	No aplica	**Tiempo**	No aplica
Procedimiento	No aplica					
Equipo	No aplica					
Personal	No aplica					
XVI.- Técnicas para la supresión y borrado seguro de los datos personales						
Datos del sistema que será cancelado: No aplica						
Denominación:	No aplica					
Motivos:	No aplica					
Plazos y condiciones para el bloqueo del sistema: No aplica						
Medidas de seguridad para el bloqueo y posterior supresión del sistema: No aplica						
Procedimiento para la supresión y período de conservación del sistema: No aplica						
Mecanismos para la supresión del sistema: No aplica						

*****NOTA: El Sistema INFOMEX y la Plataforma Nacional de Transparencia (PNT), no son administradas por este Sujeto Obligado.

Recursos de Revisión

Unidad Administrativa: Coordinación de la Unidad de Transparencia e Información			
I.- Nombre del sistema:	Recursos de Revisión		
II.- Nombre cargo y adscripción del administrador del sistema **III.- funciones y obligaciones de las personas que traten datos personales.**			
Administrador Responsable			
Nombre:	Beatriz Adriana Hernández Portillo	**Cargo**:	Coordinadora de la Unidad de Transparencia e Información
Funciones: • Coordinar y dirigir la recepción y trámite a las solicitudes de acceso a la información recibidas de forma personal o a través del Sistema Infomex. • Supervisar la canalización de las peticiones de la información solicitada a las áreas correspondientes y dar respuesta en tiempo y forma a las solicitudes de información. • Diseñar, proponer e implementar programas de acción y asistencia a los particulares en la elaboración de solicitudes de acceso a la información. • Implementar y vigilar los mecanismos de registro y control de solicitudes de acceso a la información. • Convocar y remitir al Comité de Transparencia la Información que requiera ser clasificada y dar seguimiento a los acuerdos o criterios emitidos en sesiones ordinarias y extraordinarias. • Supervisar el registro de acuerdos o criterios emitidos por el Comité de Transparencia. • Remitir el informe al ITEI respecto de la información solicitada a la FECC. • Diseñar e implementar capacitación constante en materia de transparencia y protección de datos para el personal. • Diseñar e implementar el cumplimiento de las medidas, controles y acciones para la protección de datos personales en la Dependencia. • Proponer y establecer al Comité de Transparencia los mecanismos correspondientes en los procedimientos internos que aseguren y fortalezcan con mayor eficiencia la gestión de solicitudes para el ejercicio de los derechos ARCO. • Las demás que le atribuyen la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios, su reglamento y la Ley de Protección de datos personales en posesión de los sujetos obligados. • Instruir el cumplimiento y seguimiento del sistema de datos personales denominado Recursos de Revisión. • Establecer los mecanismos de control que aseguren la administración óptima y la adecuada operación del Sistema de Recursos de Revisión. • Instruir el establecimiento de los parámetros y medidas de seguridad que debe contener el catálogo.			
Obligaciones: • Proteger los datos personales en posesión. • Tratar los de datos personales cuando sea exclusivamente en observancia a las facultades o atribuciones que la normatividad aplicable. • Vigilar y supervisar que se lleve a cabo el correcto resguardo de datos personales.			
Usuario Responsable 1			
Nombre:	Margarita Ramírez Esparza	**Cargo**:	Analista Digitalizador de Transparencia
Funciones y Obligaciones: • Recibir y dar trámite a las solicitudes de acceso a la información realizando los trámites internos necesarios para obtener la información solicitada y así estar en posibilidades de otorgar una respuesta en tiempo y forma al solicitante. • Asistir a los particulares en la elaboración de solicitudes, y en su caso, orientarlos sobre los sujetos obligados que pudieran tener la información que solicitan. • Realizar y remitir el informe al Instituto de Transparencia e Información Pública del Estado de Jalisco sobre las respuestas de negativa o afirmativa parcial respecto de la información solicitada. • Realizar un control de registro de solicitudes de acceso a la información, sus resultados y costos. • Apoyar en la logística y organización de sesiones a cargo de la Coordinación, así como en las demás tareas inherentes a dicha logística. • Remitir al Comité de Clasificación de información Pública de esta Institución la información que por su naturaleza requiera ser clasificada y llevar a cabo el registro de acuerdos o criterios emitidos por dicho Comité. • Apoyar en la promoción de la cultura de la transparencia y el acceso a la información pública al interior de la FECC.			

• Auxiliar al Titular de la Unidad de Transparencia para asesorar al Fiscal Especializado y a los Titulares de las Unidades Administrativas con relación al ejercicio del derecho a la protección de datos personales. • Coadyuvar en la realización de procedimientos internos y la elaboración de respuestas de solicitudes para el ejercicio de los derechos ARCO a fin de dar cumplimiento a lo estipulado y normatividad aplicable vigente en la materia. • Diseñar e implementar en coordinación con las área o unidades administrativas competentes, el cumplimento de las medidas, controles y acciones para la protección de datos personales. Así como proponer mecanismos para asegurar que los datos personales solo se entreguen a su titular o sus representantes debidamente acreditados. • Las demás que le atribuyan la Ley de Transparencia y acceso a la información Pública del Estado de Jalisco y sus Municipios, su reglamento y la Ley de protección de datos personales en posesión de sujetos obligados. • Realizar el debido manejo de la información que integra el Sistema de Recursos de Revisión.						
Obligaciones: • Proteger los datos personales en posesión. • Tratar los de datos personales cuando sea exclusivamente en observancia a las facultades o atribuciones que la normatividad aplicable. • Vigilar y supervisar que se lleve a cabo el correcto resguardo de datos personales.						
Encargado						
Nombre:	No aplico		**Cargo**:	No aplica		
Funciones y Obligaciones: No aplica						
IV.- Inventario de datos personales **V.- Estructura y descripción de los sistemas**						
Ordinarios:	Identificativos: nombre, domicilio, teléfono particular, teléfono celular, firma, nacionalidad, rango edad, escolaridad y ocupación.					
Sensibles:	No aplica					
Quién suministra	De forma personal, directamente del titular e indirectamente del titular					
Cómo suministra	Formato físico, formularios electrónicos, correo electrónico					
Finalidad:	Dar respuesta a los Recursos de Revisión derivados de solicitudes de acceso a la información pública					
Tipo de Soporte	**Físico**	Sí	**Electrónico**	Sí	**Otro:**	No
	Descripción		Físico: Expediente numerado de la solicitud. Electrónico: Base de datos en hoja de cálculo.			
	Características del lugar donde se resguardan		Archivero y Computadora			
Participación en el ciclo de vida del dato personal	Obtención, conservación, utilización, transferencia y almacenamiento.					
VI.- Controles y Mecanismos de Seguridad de las transferencias **VII.- Resguardo de los Sistemas** **VIII.- Bitácoras para accesos y operación cotidiana** **XII.- Medidas de seguridad aplicadas a las instalaciones** **XIII.- Controles de identificación y autenticación de los usuarios**						
Nivel de seguridad	Básico	x	Medio	x	Alto	x
Transferencias de datos personales						
Transferencia Electrónico y digital:	**Web service**	No aplica	**Web Transfer**	Sí	**Nube**	No aplica
	Discos externos	No aplica	**Carpetas compartidas**	No aplica	**CD**	No aplica
	Correo	Sí	**USB**	No aplica	**Otro:**	Infomex, PNT
Medidas de seguridad transferencia electrónica digital	cifrado https. En plataforma nacional de transparencia y sistema Infomex					
Transferencia Físico	Notificaciones al ITEI					
Medidas de seguridad transferencia física	Personal autorizado y acuse de recibo					
Almacenamiento Sistemas de Datos Personales						
	Servidor	No aplica	**Computadora**	Sí	**Nube**	No aplica

Almacenamiento Electrónico y digital:	**Discos externos**	No aplica	**Carpetas compartidas**	No aplica	**CD**	No aplica
	Correo	Sí	**USB**	Sí	**Otro:**	Infomex, PNT
Medidas de seguridad almacenamiento electrónica digital	Clave de acceso a sistemas, usuario, clave de acceso a la plataforma nacional y sistema Infomex, sistema de firewall, antivirus, contraseñas para acceder a las computadoras, sistemas de bloqueo de pantalla cada 5 minutos en las computadoras					
Almacenamiento Físico	Expedientes consecutivos					
Medidas de seguridad almacenamiento física	Archiveros y puertas con chapa para accesar a la Unidad de Transparencia					
Acceso a las instalaciones						
Seguridad perimetral exterior: Resguardo policial, cámaras de seguridad y puerta con llave						
Seguridad perimetral interior: Puerta con llave						
Bitácoras para accesos y operación cotidiana						
Los datos que se registran en las bitácoras: Número de Expediente, Fecha de ingreso, Nombre del recurrente, Solicitud, Medio de presentación, Folio, Fecha de término, Fecha de Respuesta, Nombre de quien responde.						
Soporte de la bitácora:	**Físico**	x	**Electrónico**	x	**Otro:**	
Lugar de almacenamiento:	Física: Unidad de Transparencia, Archivero. Electrónica: Computadora Base de datos en hoja de cálculo.		**Tiempo**	3 años		
Como se asegura la integridad:	Físico: Acceso a personal autorizado. Electrónico: Acceso solo al resguardante de computadora con contraseña					
XI.- Gestión de Vulneraciones						
Datos que se registran: No se tiene						
Soporte del registro:	**Físico**	No aplica	**Electrónico**	No aplica	**Otro:**	No aplica
Lugar de almacenamiento:	No aplica		**Tiempo**	No aplica		
Como se asegura la integridad:	No aplica					
XIV.- Respaldo y recuperación de datos						
Tipo de respaldo:	**Completo**	x	**Diferencial**		**Incremental**	
Medios para almacenar copias de seguridad	Documento electrónico					
XV.- Plan de Contingencia						
Se cuenta con Plan de contingencia			Si		No	x
Se realizan pruebas de eficiencia			Si		No	x
Se cuenta con un sitio redundante			Si		No	x
Tipo de sitio :	**Caliente**	No aplica	**Tibio**	No aplica	**Frío**	No aplica
	Propio	No aplica	**Subcontratado**	No aplica	**Tiempo**	No aplica
Procedimiento	No aplica					
Equipo	No aplica					
Personal	No aplica					
XVI.- Técnicas para la supresión y borrado seguro de los datos personales						
Datos del sistema que será cancelado: No aplica						
Denominación:	No aplica					
Motivos:	No aplica					
Plazos y condiciones para el bloqueo del sistema: No aplica						
Medidas de seguridad para el bloqueo y posterior supresión del sistema: No aplica						
Procedimiento para la supresión y período de conservación del sistema: No aplica						
Mecanismos para la supresión del sistema: No aplica						

*****NOTA: El Sistema INFOMEX y la Plataforma Nacional de Transparencia (PNT), no son administradas por este Sujeto Obligado.

Análisis de Riesgo

El presente análisis de riesgo se realizó con apoyo en la *Metodología de Análisis de Riesgo BAA*, instrumento publicado por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, en el mes de marzo del año 2014, que tiene como objetivo final determinar los controles recomendados de protección de datos de acuerdo con el entorno de riesgo existente.

La metodología de análisis de riesgos que se presenta en este documento se enfoca en tres variables que afectan la percepción del valor de los datos personales para un atacante:

1) Beneficio para el atacante. Aquellos datos personales que representen mayor beneficio tienen más probabilidad de ser atacados (Riesgo por tipo de dato).

2) Accesibilidad para el atacante. Aquellos datos personales que sean de fácil acceso tienen mayor probabilidad de ser atacados (Nivel de accesibilidad).

3) Anonimidad del atacante. Aquellos datos personales cuyo acceso represente mayor anonimidad tienen más probabilidad de ser atacados (Nivel de anonimidad).[1]

[1] Metodología de Análisis de Riesgo BAA, Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, marzo del 2014.

Análisis de Riesgo

Inventario de datos personales	Tipo de dato	Nivel de Riesgo inherente	Volumen de Titulares	Nivel de Riesgo por Tipo de Dato (beneficio)	Accesibilidad (cantidad de accesos a datos personales	Entorno	Nivel de por Tipo de Entorno (anonimidad)	Patrones de control
Registro de Visitas	Se oculta esta información debido a que contiene el análisis de los Sistemas de Información Confidencial, y se establece los niveles de riesgo señalados en el encabezado de esta tabla, de acuerdo a los parámetros precisados en la siguiente página. Lo cual se traduce en información relevante que puede ser aprovechada para los fines contrarios al presente documento.							
Registro de Documentos								
Integración de Carpetas de Integración								
Procesos de Compras								
Contratación de personal								
Solicitudes de Acceso a Información Pública								
Solicitudes de Ejercicio de Derechos ARCO								
Recursos de Transparencia								
Recursos de Revisión								

Equivalencias

Nivel de riesgo inherente

Tipo de Dato	Nivel de Riesgo Inherente
Ubicación en conjunto con patrimoniales	REFORZADO
Información adicional de tarjeta bancaria	REFORZADO
Titulares de alto riesgo	REFORZADO
Salud	ALTO
Origen, creencias e ideológicos	ALTO
Ubicación	MEDIO
Patrimoniales	MEDIO
Autenticación	MEDIO
Jurídicos	MEDIO
Tarjeta Bancaria	MEDIO
Personales de identificación	BAJO

Fuente: Metodología de Análisis de Riesgo BAA, INAI, marzo del 2014

Umbrales de nivel de accesibilidad

Accesibilidad (cantidad de accesos a los datos personales)
≤ 20
>20 ≤ 200
>200 ≤ 2,000
>2,000

Fuente: Metodología de Análisis de Riesgo BAA, INAI, marzo del 2014

Nivel de riesgo por tipo de dato

Tipo de Dato	Nivel de Riesgo Inherente	Volumen de Titulares				
		<500k	<5k	<50k	<500k	>500k
Ubicación en conjunto con patrimoniales	REFORZADO	4	4	5	5	5
Información adicional de tarjeta bancaria	REFORZADO	4	4	5	5	5
Titulares de alto riesgo	REFORZADO	4	4	5	5	5
Salud	ALTO	1	2	3	3	3
Origen, creencias e ideológicos	ALTO	1	2	3	3	3
Ubicación	MEDIO	1	1	2	3	3
Patrimoniales	MEDIO	1	1	2	3	3
Autenticación	MEDIO	1	1	2	3	3
Jurídicos	MEDIO	1	1	2	3	3
Tarjeta Bancaria	MEDIO	1	1	2	3	3
Personales de identificación	BAJO	1	1	1	1	1

Fuente: Metodología de Análisis de Riesgo BAA, INAI, marzo del 2014

Nivel de anonimidad

Entorno	Nivel de Anonimidad
Físico	1
Red interna	2
Red inalámbrica	3
Red de terceros	4
Internet	5

Fuente: Metodología de Análisis de Riesgo BAA, INAI, marzo del 2014

Análisis de Riesgo de acuerdo a Amenazas y Vulnerabilidades.

Se considera como activo a la información, el conocimiento sobre los procesos, el personal, hardware, software y cualquier otro recurso involucrado en el tratamiento de los datos personales, que tiene valor para la FECC.

Tipo de activo	Tipo de activo de apoyo
Información (datos personales).	Hardware (computadora de escritorio y portátil).
	Software (sistema operativo, licencias de usuario, sistemas de administración de personal y nómina).
	Soporte (Físico: papel, fotografía, entre otros. Electrónico: dispositivos de almacenamiento externo, cd, usb, entre otros).
	Redes y telecomunicaciones (wifi, router, entre otros).
	Personal

En la siguiente tabla se describen las amenazas a los datos personales que trata la FECC, de origen humano (provocados intencionalmente):

Origen de la amenaza	Causa	Posibles consecuencias
Hacker, cracker,	Se oculta esta información, ya que representa un riesgo potencial para la protección de los datos personales en resguardo la Fiscalía Especializada en Combate a la Corrupción.	
Criminal computacional		
Espía		
Personal		

En la siguiente tabla se describen las amenazas a los datos personales que trata la FECC, por causas fortuitas (no intencionales):

Tipo	Amenazas
Daño Físico	Se oculta esta información, ya que representa un riesgo potencial para la protección de los datos personales en resguardo la Fiscalía Especializada en Combate a la Corrupción
Eventos Naturales	
Pérdida de Servicios Básicos	
Información comprometida por fallas técnicas	
Acciones no Autorizadas	
Compromiso de las Funciones	

En la siguiente tabla se presentan escenarios de incidente, donde se muestran amenazas que podrían explotar una vulnerabilidad.

Tipo de Activo	Vulnerabilidades	Amenazas	Posible vulneración a los datos personales
Hardware	Se oculta esta información, ya que representa un riesgo potencial para la protección de los datos personales en resguardo la Fiscalía Especializada en Combate a la Corrupción		
Software			
Redes			

	Se oculta esta información, ya que representa un riesgo potencial para la protección de los datos personales en resguardo la Fiscalía Especializada en Combate a la Corrupción
Personal	
Sitio	
Organización	

	Se oculta esta información, ya que representa un riesgo potencial para la protección de los datos personales en resguardo la Fiscalía Especializada en Combate a la Corrupción

Análisis de Brecha

El análisis de brecha consiste en identificar:

Medidas básicas de seguridad para accesos físicos

- Las medidas de seguridad existentes

Control	Parámetro	Carácter
Se oculta esta información, ya que representa un riesgo potencial para la protección de los datos personales en resguardo la Fiscalía Especializada en Combate a la Corrupción		

- Las medidas de seguridad existentes que operan correctamente

Control	Parámetro	Carácter
Se oculta esta información, ya que representa un riesgo potencial para la protección de los datos personales en resguardo la Fiscalía Especializada en Combate a la Corrupción		

- Las medidas de seguridad faltantes

Control	Parámetro	Carácter
Se oculta esta información, ya que representa un riesgo potencial para la protección de los datos personales en resguardo la Fiscalía Especializada en Combate a la Corrupción		

- Si existen nuevas medidas de seguridad que puedan remplazar a uno o más controles implementados actualmente.

Actualmente no existen nuevas medidas de seguridad

Medidas reforzadas de seguridad para accesos físicos

- Las medidas de seguridad existentes

Control	Parámetro	Carácter
Se oculta esta información, ya que representa un riesgo potencial para la protección de los datos personales en resguardo la Fiscalía Especializada en Combate a la Corrupción		

- Las medidas de seguridad existentes que operan correctamente

Control	Parámetro	Carácter
Se oculta esta información, ya que representa un riesgo potencial para la protección de los datos personales en resguardo la Fiscalía Especializada en Combate a la Corrupción		

- Las medidas de seguridad faltantes

Control	Parámetro	Carácter
Se oculta esta información, ya que representa un riesgo potencial para la protección de los datos personales en resguardo la Fiscalía Especializada en Combate a la Corrupción		

- Si existen nuevas medidas de seguridad que puedan remplazar a uno o más controles implementados actualmente.
Actualmente no existen nuevas medidas de seguridad

Lista de medidas administrativas para nivel 4 y 5

- Las medidas de seguridad existentes

Control	Parámetro	Carácter
Se oculta esta información, ya que representa un riesgo potencial para la protección de los datos personales en resguardo la Fiscalía Especializada en Combate a la Corrupción		

Se oculta esta información, ya que representa un riesgo potencial para la protección de los datos personales en resguardo la Fiscalía Especializada en Combate a la Corrupción

- Las medidas de seguridad existentes que operan correctamente

Control	Parámetro	Carácter
Se oculta esta información, ya que representa un riesgo potencial para la protección de los datos personales en resguardo la Fiscalía Especializada en Combate a la Corrupción		

Se oculta esta información, ya que representa un riesgo potencial para la protección de los datos personales en resguardo la Fiscalía Especializada en Combate a la Corrupción

- Las medidas de seguridad faltantes

Control	Parámetro	Carácter
Se oculta esta información, ya que representa un riesgo potencial para la protección de los datos personales en resguardo la Fiscalía Especializada en Combate a la Corrupción		

- Si existen nuevas medidas de seguridad que puedan remplazar a uno o más controles implementados actualmente.

Actualmente no existen nuevas medidas de seguridad.

Los mecanismos de monitoreo y revisión de las medidas de seguridad

Se llevará a cabo monitoreo y revisión de los riesgos con sus factores relacionados, es decir, el valor de los activos, las amenazas, vulnerabilidades, el impacto, y la probabilidad de ocurrencia, para identificar en una etapa temprana cualquier cambio en el contexto del alcance y objetivos del Documento de Seguridad de la FECC.

La FECC asegurará que los siguientes puntos estén continuamente monitoreados:

- Nuevos sistemas de tratamiento de datos personales que se incluyan en los alcances de la gestión de riesgo.
- Modificaciones necesarias a los datos personales.
- Nuevas amenazas que podrían estar activas dentro y fuera de la FECC y que no han sido valoradas.
- La posibilidad de que vulnerabilidades nuevas o incrementadas sean explotadas por las amenazas correspondientes.
- Vulnerabilidades identificadas para determinar aquéllas expuestas a amenazas nuevas o pasadas que vuelven a surgir.
- Cambio en el impacto o consecuencias de amenazas valoradas, vulnerabilidades y riesgos en conjunto, que resulten en un nivel inaceptable de riesgo.
- Incidentes y vulneraciones de seguridad.

Los factores que determinan la probabilidad de ocurrencia y consecuencias podrían cambiar, lo que afectaría la conveniencia y costos de las opciones de tratamiento. Los cambios mayores que afectan a la organización deben ser revisados de manera específica, no obstante que las actividades de monitoreo requieren de regularidad y periodicidad.

Auditoría

Se realizará una auditoría interna anual para monitorear y revisar la eficacia y eficiencia del Documento de Seguridad, así como las Políticas de Seguridad de la Información. Esta supervisión se planeará, establecerá y mantendrá tomando en cuenta la política de gestión de datos personales, misma que tendrá como objetivo, lo siguiente:

a) Evaluar el cumplimiento de las unidades administrativas de la FECC a sus obligaciones en materia de protección de datos personales;
b) Vigilar el adecuado tratamiento de datos personales que llevan a cabo las unidades administrativas de la FECC.

El plan de trabajo

La Unidad de Transparencia es instancia que funge como vínculo entre la FECC como responsable del tratamiento de datos personales y el titular de los datos personales y vigilar el cumplimiento de las obligaciones que tiene como Sujeto Obligado sean cumplidas cabalmente.

Este Plan consiste en plasmar el trabajo y actividades que la Unidad de Transparencia realizará durante el año 2019, a fin de que sean cumplidas las obligaciones que le devienen de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios.

Objetivos generales

1. Garantizar la protección de datos personales en cumplimiento de la normatividad.

2. Contribuir al fortalecimiento de la cultura de la Protección de Datos.

Estrategias

1. Establecer mecanismos de sensibilización para los servidores públicos que laboran en la FECC sobre la importancia de la protección de los datos personales.

2. Desarrollar e implementar políticas para el resguardo y protección de los datos personales de acuerdo a los principios, deberes y obligaciones en la materia, establecidos en la normatividad aplicable.

Acciones para el mejoramiento del desempeño

Estrategia 1

Duración: de agosto 2019 a septiembre 2019

Objetivo: Salvaguardar el derecho a la protección de los datos personales de las personas, así como el ejercicio de los derechos de acceso, rectificación, cancelación y oposición al tratamiento de los datos personales (ARCO).

Áreas involucradas: Todas las áreas.

Acciones:

- Capacitar al personal en materia de derecho de datos personales, principios, deberes, responsabilidades y sanciones.
- Desarrollar e implementar los mecanismos de gestión de las solicitudes de derechos ARCO.
- Capacitación sobre los derechos ARCO a las unidades administrativas internas.

- Atender las solicitudes de acceso a la información pública en forma lo más antes posible.
- Atención de los recursos de revisión en datos personales.

Estrategia 2

Duración: de septiembre 2019 a diciembre 2019

Objetivo: Proteger los datos personales de posibles amenazas y vulneraciones que pueden sufrir los mismos.

Áreas involucradas: Todas las áreas.

Acciones:

- Vigilar que los datos se traten conforme a legislación aplicable.
- Contar con un Aviso de Privacidad actualizado y que cumpla con los requisitos establecidos en la norma, que pueda estar al alcance y entendimiento de los titulares de la información.
- Revisar que los datos recabados por las áreas sean proporcionales a los fines para los cuales se están recabando.
- Contar con los mecanismos para procurar que los datos personales sean exactos, completos, pertinentes actualizados y correctos.
- Establecer procedimientos para corregir y actualizar los datos personales.
- Establecer procedimientos para la conservación, bloqueo y supresión de los datos personales.
- Elaboración de Documento de Seguridad: La elaboración de un documento que contenga las medidas de seguridad de carácter físico, técnico y administrativo conforme a la Ley, el cual será actualizado de manera periódica.
- Elaboración de acuerdos de transferencia previo aviso de las áreas que transfieran los datos personales en posesión de la FECC a otro sujeto obligado.

El programa general de capacitación.

Nombre: Programa de capacitación de la Unidad de Transparencia de la FECC 2019.

Justificación
La capacitación no solo es necesaria para tener conocimiento de la norma, sino también para sensibilizar a los servidores públicos en la protección de los datos personales; además que, de conformidad con los artículos 29 fracción III y 87 fracción VII de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios, existe la obligación de poner en práctica un programa de capacitación y actualización del personal sobre las obligaciones y demás deberes en materia de protección de datos personales

El presente programa de capacitación es de aplicación para todos los servidores públicos que trabajan en la FECC y tiene los siguientes objetivos:

- Sensibilizar a los trabajadores de la FECC en materia de protección de los datos personales.
- Contar con personal capacitado en materia de protección de los datos personales.

Meta
Capacitar al 100% de los servidores públicos que resguardan información o que tratan datos personales dentro del sujeto obligado.

Estrategia
- Realización de talleres, sesiones de capacitación internas.
- Metodología de exposición (Diálogo).

Cronograma

FECHA	SEDE	TEMA
13/09/2019	Sala de Juntas de la FECC	Medidas de seguridad de la información
27/09/2019		Medidas de seguridad de la Información
11/10/2019		Datos personales: principios, deberes, responsabilidades, sanciones y Derechos ARCO
25/10/2019		Datos personales: principios, deberes, responsabilidades, sanciones y Derechos ARCO

*Las fechas y el lugar de la capacitación están sujetas a cambios, el personal a capacitarse se convocará, cuando menos, con tres días de anticipación.