



EDUCACIÓN

DOCUMENTO DE SEGURIDAD PARA LA PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE LA SECRETARIA DE EDUCACIÓN DEL ESTADO DE JALISCO.

OBJETIVO.

Este documento es de orden obligatorio y asegura la integridad, la confidencialidad y disponibilidad de los datos e información personal que se encuentran en posesión de la Secretaría de Educación del Estado de Jalisco, en su carácter de Sujeto Obligado. Del mismo modo delimita las obligaciones de los responsables, encargados y usuarios de cada sistema y las medidas de seguridad administrativa, fiscal y técnica que deberán implementarse para el correcto manejo de la información que se posee. Lo anterior de conformidad a la Ley General de Protección de Datos Personales, la Ley de Protección de Datos Personales del Estado de Jalisco y sus Municipio, así como de lo señalado por la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipio.

El presente documento fue elaborado por la Unidad de Transparencia y aprobado en su totalidad por el Comité de Transparencia, ambos de este sujeto obligado, mismo que será de observancia obligatoria para todos los servidores públicos de la dependencia, así como para las personas externas que



EDUCACIÓN

debido a la prestación de algún servicio deba tener acceso a información, sistema, o sitio web en el que se ubique cualquier tipo de dato personal protegido por esta Secretaría.

LA SECRETARÍA DE EDUCACIÓN DEL ESTADO DE JALISCO Y COMITÉ DE TRANSPARENCIA

La Secretaría de Educación del Estado de Jalisco, a través del Comité de Transparencia aprueba el presente Documento de Seguridad, el día 30 de agosto de 2018, lo anterior con fundamento en lo dispuesto por los artículos 35 de la Ley General de Protección de Datos Personales; artículo 3, fracción XIV, 5, 35, 36, 37, 38 39 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus municipios, así como lo previstos en el artículo 3 de la Ley de Transparencia e Información Pública del Estado de Jalisco y el primero, segundo, tercero, décimo segundo, décimo quinto, décimo sexto, vigésimo quinto, vigésimo sexto, vigésimo octavo vigésimo noveno, Trigésimo, Cuadragésimo segundo, Cuadragésimo quinto, Cuadragésimo sexto, de los Lineamientos generales para el manejo, mantenimiento, seguridad y protección de la información confidencial y el artículo 28 del Código Civil del Estado de Jalisco.

SOBRE EL DOCUMENTO DE SEGURIDAD.

El presente documento se refiere al instrumento que describe y da cuenta de manera general sobre las medidas de seguridad, técnicas, físicas y administrativas que ha adoptado la Secretaría de Educación del Estado de Jalisco, para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que poseemos.

QUE SON LOS DATOS PERSONALES

Los datos personales, así como la 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 cual información. Tales como el nombre, domicilio, números telefónicos, números de seguridad social, relativas al patrimonio, las que se refiera a sus características físicas, morales o emocionales, a su vida afectiva o familiar, entre otros.

También existen los Datos Personales Sensibles, que son aquellos que se refieren a la esfera íntima de su titular, o cuya utilización indebida puede dar origen a discriminación o conlleve un riesgo grave para éste. Tales como los relativos a su origen étnico o racial, estado de salud, información genética, datos biométricos, creencias religiosas, filosóficas y morales, opiniones políticas y preferencias sexuales u otros similares.¹

Es de destacar que, en el tratamiento de los datos personales de los menores de edad, se deberá de privilegiar el interés superior de la niña, el niño y el adolescente, en términos de las disposiciones aplicables.²

Esta autoridad deberá de registrarse y actuar bajo los principios enunciados en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco, de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información, y responsabilidad.

SOBRE EL AVISO DE PRIVACIDAD.

Si los ciudadanos o instituciones privadas, proporcionan a la Secretaría de Educación información confidencial, esta deberá de dar a conocer las políticas respecto de su protección, de conformidad con lo señalado por la Ley de Protección de Datos del Estado, los lineamientos que establezca el Instituto de Transparencia e Información Pública y Protección de Datos Personales del Estado de Jalisco, lo anterior de conformidad al Aviso de Privacidad, que especifica las medidas que ha tomado la Secretaría para garantizar la seguridad en el tratamiento de los datos personales que se recaban con motivo de tramites o del desempeño propio de las labores de este sujeto obligado, a través del cual se evita su alteración, pérdida, transmisión, publicación y acceso no autorizado.

¹ Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco artículo 3 fracción IX y X

² Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco artículo 5, numeral 3.



SOBRE LOS DERECHOS ARCO

Se trata de solicitudes sobre los datos personales que posee el sujeto obligado, sobre los cuales se ejercen los derechos al Acceso, Rectificación, Cancelación y Oposición de los mismos, las cuales podrá realizar solamente el titular de los datos personales o su representante legal.

Resulta necesario acotar que, por razones de seguridad y protección de los datos personales, que este sujeto obligado pose, es necesario que, para cualquier trámite relacionado al ejercicio de los Derechos ARCO, la identificación plena del solicitante, a través de los medios legales establecidos para ellos, (credencial INE, pasaporte vigente, cédula profesional, cartilla militar) tanto para solicitar como para recibir la información solicitada.

Es importante destacar que la única instancia facultada para el tratamiento de los Datos Personales dentro de la Secretaría de Educación, es el Comité de Transparencia mismo que entrará al estudio y evaluará la procedencia de las mismas de conformidad con la normativa nacional y estatal vigente, así como en base a los lineamientos dispuestos por el Instituto de Transparencia. El Comité de Transparencia. Este deberá realizar una resolución debidamente fundada y motivada la que será notificada al solicitante, respecto de la solicitud de cualquiera de los Derechos ARCO.

EL TRATAMIENTO DE LA INFORMACIÓN POR PARTE DE LOS SUJETOS OBLIGADOS

Los sujetos obligados deberán adoptar medidas necesarias para el debido tratamiento, manejo, mantenimiento, seguridad y protección de la información confidencial que obre en su poder, así como los procedimientos necesarios para garantizar la protección, tratamiento, mantenimiento, seguridad sobre el destino final de los datos personales que posean con motivo de sus atribuciones.

Es necesario comprender que el tratamiento de datos personales, debe versar sobre toda aquella información que pueda encontrarse en cualquier material ya sea en documento o medios digitales, como fotografías, grabaciones, soporte magnético, digital, sonoro, visual, electrónico, informático u otro elemento análogo.

Solo podrán tener acceso a la información confidencial en posesión de este sujeto obligado, los miembros del Comité, el titular de la UTI, el responsable o los usuarios



quienes por las labores que desempeñan, deban de tener acceso a dicha información.

Además de ello, todos los datos personales que sean recabados por esta autoridad educativa, a través de cualquier medio, deberá sujetarse a lo dispuesto por anteriormente dispuesto y deberán ser tratados exclusivamente para la finalidad que fueron obtenidos.

DE LOS SISTEMAS DE TRATAMIENTO Y BASES DE DATOS PERSONALES CON LOS QUE CUENTA LA SECRETARIA DE EDUCACIÓN DE EDUCACIÓN DEL ESTADOS DE JALISCO

La Secretaria de Educación al ser una institución encargada de la administración Educación del Estado de Jalisco y por la naturaleza de las funciones conferidas, cuenta con diversos sistemas y bases de datos, que cuentan con datos personales, sobre los que versa una doble responsabilidad, pues en su mayoría corresponden a datos de menores de edad, por lo que el tratamiento que debe darse a estos, debe atender en todo momento al bien superior de las niñas, los niños y adolescentes, en ese sentido, debemos entender que la información académica y de ubicación de menores, tiene el carácter de reservada, por lo que los estándares de seguridad que deberá aplicar este sujeto, deberán ser los de más alta seguridad y protección, basados en todos aquellos de carácter nacional e internacional, necesarios para tal fin.

Así mismo esta Secretaria cuanta con datos referentes a información laboral de administrativos y docentes, la cual deberá ser tratada con el mismo sigilo y de conformidad con las medidas de seguridad necesarias y establecidas en la normativa vigente.

A continuación, se enlistan los sistemas y bases de datos con los que cuanta este sujeto obligado, los cuales son de orden interno, y no son considerados fuentes de acceso público, ya que los mismos son necesarios para realizar las funciones sustantivas de esta dependencia, el listado no corresponde a lista de importancia:

- I.- Becas Jalisco, de la Dirección de Becas;
- II.- Becas de Escuelas Particulares, de la Dirección de Becas;
- III.- Becas de Educación Superior, de la Dirección de Becas;
- IV.- Bolsa de Trabajo, de la Dirección General de Recursos Humanos;



EDUCACIÓN

- V.- Asignación de Plazas, de la Dirección General de Recursos Humanos;
- VI.- Centros de Atención y Servicio (CAS), de la Dirección de CAS;
- VII.- Gestión escolar;
- VIII.- SIPAS, de la Dirección de Participación Social;
- IX.- ME CUIDA, Dirección General de Equidad;
- X.- MISIONES CULTURALES;
- XI.- Control escolar de Normales, de la Dirección General de Normales
- XII.- Redes y Telecomunicaciones, de DDTI;
- XIII.- Solicitudes de Información, Unidad de Transparencia;
- XIV.- Solicitudes de Derechos ARCO, Comité de Transparencia;
- XV.- BPN Financieros, Dirección General de Control Financiero y Contable;
- XVI.- Agenda del Secretario, Despacho del Secretario;
- XVII.- Refrendo de Preescolares Particulares, Dirección de Preescolar;
- XVIII.- Mi escuela, Coordinación de Educación Básica;
- XIX.- CAM, Formación para el Trabajo, Centros de Formación para el Trabajo;
- XX.- SIAPSEP-SIAN-RH, de la Dirección de Recursos Humanos y DRSES
- XXI.- Gestión Educativa, Coordinación de Planeación, DRSES, Escuelas;
- XXII.- SCEJAL, Coordinación de Planeación, DRSES, Escuelas.

DE LOS RESPONSABLES Y ENCARGDOS DE LA PROTECCIÓN DE LOS DATOS PERSONALES E INFORMACIÓN CONFIDENCIAL.

Comité de Transparencia, la Unidad de Transparencia, así como los titulares de las diferentes áreas que tengan a su cargo el resguardo de información que contenga Datos Personales, serán los responsables de resguardarla, así como promover las medidas necesarias para su tratamiento y custodia.



Por su parte el Comité de Transparencia, con ayuda de la Unidad de Transparencia, se encargará de establecer la información que tenga carácter de confidencial o reservada.

- Dictará las medidas necesarias para el tratamiento que deba darse a los datos personales de menores de edad, privilegiando siempre el interés superior de la niña, el niño y el adolescente, en los términos de las disposiciones legales aplicables. Entendiendo que, en todo momento y como política institucional, toda la información referente a estos, tiene el carácter de reservada, salvo que se dicte disposición en contrario por autoridad competente, para el caso concreto o quien solicite información sea el padre o tutor del menor en pleno uso de sus derechos filiales, en cuyo caso el único autorizado para determinar el acceso a los datos, será evaluado por el Comité de Transparencia.

MEDIDAS DE SEGURIDAD

Se trata de todas aquellas medidas que adopta el Comité de Transparencia de la Secretaría y en su caso, en conjunto con el área que los posea, siempre que sea necesario, para asegurar que la información confidencial y los datos personales sean resguardados, de manera íntegra, segura y adecuada, ya sea a través de mecanismos administrativos, técnicos, físicos, políticas de procesos, controles.

De conformidad con lo señalado por la Ley de protección de Datos Personales, los deberes sobre la Seguridad de los datos personales, debe entenderse de la siguiente forma:

"Con independencia del tipo de sistema en el que se encuentren los datos personales o el tipo de tratamiento que se efectúe, el responsable deberá establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales, que permitan protegerlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad; sin perjuicio de lo establecido por las disposiciones vigentes en materia de seguridad emitidas por las autoridades competentes al sector que corresponda, cuando éstas contemplen una protección mayor para el titular o complementen lo dispuesto en esta Ley y demás disposiciones aplicables".

Dentro de las medidas de seguridad tenemos las señaladas por la Ley de Protección de Datos del Estado y se deben de seguir cuando menos lo elementos ahí señalados:



"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. De manera enunciativa más no limitativa, se debe considerar las siguientes actividades:

- a) Prevenir el acceso no autorizado al perímetro de la organización, sus instalaciones físicas, áreas críticas, recursos e información;
- b) Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, recursos e información;
- c) Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico, que pueda salir fuera de las instalaciones de la organización; y
- d) Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz que asegure su disponibilidad, funcionalidad e integridad.

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. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades:

- a) Prevenir que el acceso a las bases de datos o a la información, así como a los recursos, sea por usuarios identificados y autorizados;
- b) Generar un esquema de privilegios para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones;
- c) Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware; y
- d) Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales.³

Con lo anterior se pretende que únicamente personal autorizado e plenamente identificado tenga acceso a los datos personales en posesión de este sujeto obligado y, así también, que el servidor público que tenga acceso a dicha

³ Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios, artículo 3, fracción XXV, XXVI, XXVII Y XXVIII.



EDUCACIÓN

información evite que ésta sea divulgada, a efecto de no comprometer la integridad, confiabilidad y disponibilidad de los sistemas de datos.

OBJETIVO DE LA IMPLEMENTACIÓN DE MEDIDAS DE SEGURIDAD SOBRE LOS DATOS PERSONALES:

Es atribución del Comité de Transparencia de la Secretaría de Educación del Estado de Jalisco establecer las recomendaciones sobre las políticas de manejo, mantenimiento, seguridad y protección de datos personales, que estén en posesión de las unidades administrativas de la dependencia, así como identificar aquellos datos que se recaban y posee, los responsables, encargados y usuarios de cada sistema interno con los que se cuenta y las medidas de seguridad concretas implementadas por este sujeto obligado.

Por lo que es necesario promover la adopción de las medidas de índole técnica y organizativa necesarias para garantizar la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, con base en estándares de seguridad internacionales;

Para lograrlo se deben de tomar en cuenta los avances tecnológicos, la naturaleza de los datos almacenados y los riesgos a que puedan estar expuestos, si provienen de la acción humana o de las condiciones físicas y ambientales, por lo que se han establecido distintos niveles de seguridad aplicables a cada categoría o tipo de datos, alojados en los sistemas de datos personales.

Los alcances que deben de tener las recomendaciones son para convertirse en propuestas y sugerencias específicas para lograr la mayor protección de datos personales, por lo que las unidades administrativas de la dependencia de esta Secretaría podrán utilizarlas como modelo a seguir y así tener una forma de seguridad sin perjuicio de que establezcan medidas adicionales que coadyuven a la mejor protección, la integridad, confidencialidad y disponibilidad de la información personal que se tiene.

El documento deberá mantenerse siempre actualizado y ser de observancia obligatoria para todos los servidores públicos de esta Secretaría, así como para las personas externas que debido a la prestación de un servicio tengan acceso a determinado sistema o al sitio donde se ubican los mismos.



DE LOS NIVELES DE SEGURIDAD

En cuanto a los niveles de seguridad que se deben tomar respecto de la información que se posee, es necesario aclarar que los mismos no se encuentran establecidos en la legislación vigente, no obstante es de gran importancia que esta Secretaría, establezca como políticas mínimas de actuación, aquellas contempladas en los estándares más altos y de mayor uso, nacional e internacionalmente y que sean tomadas como base para el tratamiento y resguardo de los datos personales con los que contamos.

En ese sentido, para este caso en particular, tomaremos como referencia, el estándar internacional ISO/IEC 27002:2005, referente a las prácticas sobre seguridad de información y que son tomadas a su vez como ejemplo por el Instituto Nacional de Transparencia en sus Recomendaciones sobre Medidas de Seguridad Aplicables a los Sistemas de Datos Personales.

Lo anterior a fin de garantizar la protección de datos personales que tengan en posesión, estableciendo personal autorizado para la protección y promover el uso responsable de las nuevas tecnologías de la información, atendiendo los principios de protección de datos.

Por lo que tomando en cuenta los criterios internacionales establecidos sobre medidas de seguridad, para el resguardo eficaz de los datos personales, al final de cada medida, se establecen niveles de seguridad, las cuales deberán observarse atendiendo a la naturaleza de la información contenida en los sistemas establecidos.

Por lo tanto, las áreas que integran la Secretaría de Educación del Estado de Jalisco aplicarán el nivel básico, medio o alto de medidas de seguridad, de acuerdo con las categorías o tipos de datos personales.

1. NIVEL BÁSICO. -

Estas medidas serán aplicables a todos los sistemas de datos personales.⁴

⁴ Recomendaciones sobre Medidas de Seguridad Aplicables a los Sistemas de Datos Personales.
https://www.gob.mx/cms/uploads/attachment/file/83122/MODELOS_Y_GU_AS_17.pdf



- **De Identificación:** Nombre, domicilio, teléfono particular, teléfono celular, correo electrónico, estado civil, firma (en cuanto ésta no resulta confidencial cuando se emita en cumplimiento de la obligación legal por las funciones que fue contratado el servidor público y deba autorizar la emisión de un documento que por sus actividades resulta necesario avalar el contenido del texto), firma electrónica, RFC, CURP, cartilla militar, lugar de nacimiento, fecha de nacimiento, nacionalidad, edad, nombres de familiares, dependientes y beneficiarios, fotografía, costumbres, idioma o lengua, entre otros.
- **Laborales:** Documentos de reclutamiento y selección, de nombramiento, de incidencia, de capacitación, puesto, domicilio de trabajo, correo electrónico institucional (contraseña e información de procesos administrativos de la bandeja de entrada), actividades extracurriculares, referencias laborales, referencias personales entre otros.

La posesión de datos personales deberá obedecer exclusivamente a las atribuciones legales o reglamentarias de cada dependencia o entidad y deberán obtenerse a través de los medios previstos, estos datos sólo deberán tratarse únicamente para la finalidad para la cual fueron obtenidos.

Cuando los datos personales se actualicen no deben de alterar la veracidad de la información que tengan y debe de ser por personal autorizado para el cumplimiento de las atribuciones de esta Secretaría.

2. NIVEL MEDIO. -

Los datos personales además de cumplir con las medidas de seguridad de nivel básico, deberán observar las marcadas con nivel medio.⁵

- **Datos Patrimoniales:** Bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos y egresos, cuentas bancarias, seguros, afores, fianzas, servicios contratados, referencias personales, entre otros.
- **Datos sobre procedimientos administrativos seguidos en forma de juicio y/o jurisdiccionales:** Información relativa a una persona que se encuentre sujeta

⁵ IBID página 14



a un procedimiento administrativo seguido en forma de juicio o jurisdiccional en materia laboral, civil, penal o administrativa.

- **Datos Académicos:** Trayectoria educativa, títulos, cédula profesional, certificados y reconocimientos, entre otros.
- **Tránsito y movimientos migratorios:** Información relativa al tránsito de las personas dentro y fuera del país e información migratoria de las personas, entre otros.

Este tipo de datos debido a la transcendencia para la intimidad, se debe evitar prejuicios por el uso que se pueda hacer con ese tipo de información siendo factores de generar graves conflictos, si no tienen el debido cuidado al manejar la información confidencial.

3. NIVEL ALTO. -

Los datos personales que contengan algún dato que se enliste deberán cumplir con las medidas de seguridad de nivel básico y medio, deberán observar las marcadas con el nivel alto.

- **Datos Ideológicos:** Creencia religiosa, ideología, filosófica, afiliación política y/o sindical, pertenencia a organizaciones de la sociedad civil y/o asociaciones religiosas, entre otros.
- **Datos de Salud:** Estado de salud, historial clínico, alergias, enfermedades, información relacionada con cuestiones de carácter psicológico y/o psiquiátrico, incapacidades médicas, intervenciones quirúrgicas, vacunas, consumo de sustancias tóxicas, uso de aparatos oftalmológicos, ortopédicos, auditivos, prótesis, entre otros.
- **La ubicación de menores de edad:** a través de sus datos académicos y toda la información que se posea de estos, toda vez que la revelación de algún dato personal puede poner en riesgo la integridad de los menores.
- **Características personales:** Tipo de sangre, ADN, huella digital, u otros análogos.
- **Características físicas:** Color de piel, color de iris, color de cabello, señas particulares, estatura, peso, complexión, discapacidades, entre otros.
- **Vida sexual:** Preferencia sexual, hábitos sexuales, entre otros.



- **Origen:** Étnico y racial.

Los niveles de protección señalados definen el mayor o menor grado de confidencialidad, disponibilidad e integridad que el sujeto obligado debe asegurar de acuerdo con la naturaleza de los datos personales que custodia, de conformidad con las siguientes definiciones:

La **confidencialidad** es asegurar que la información no sea accedida por – o divulgada a – personas o procesos no autorizados.

La **integridad** es garantizar la exactitud y la confiabilidad de la información y los sistemas de manera que éstos no puedan ser modificados sin autorización, ya sea accidental o intencionadamente.

La **disponibilidad** es que las personas o procesos autorizados accedan a los activos de información cuando así lo requieran.⁶

ACCESOS CONTROLADOS Y BITÁCORAS

Deberá guardarse como mínimo los datos completos del responsable, encargado o usuario, el modo de autenticación del Responsable, encargado o usuario, fecha y hora en que se realizó el acceso, o se intentó el mismo, sistema de datos personales accedido, operaciones o acciones llevadas a cabo dentro del sistema de datos personales, fecha y hora en que se realizó la salida del sistema de datos personales.⁷

OPERACIONES DE ACCESO, ACTUALIZACIÓN, RESPALDO Y RECUPERACIÓN.

Se debe de contar con manuales de procedimientos y funciones para el tratamiento de datos personales que deberán observar obligatoriamente los Responsables, encargados o usuarios de los sistemas de datos personales.⁸

Llevar control y registros del sistema de datos personales en bitácoras que contengan la operación cotidiana, respaldos, usuarios, incidentes y accesos, así

⁶ Recomendaciones sobre Medidas de Seguridad Aplicables a los Sistemas de Datos Personales.
https://www.gob.mx/cms/uploads/attachment/file/83122/MODELOS_Y_GU_AS_17.pdf

⁷ GUIA PARA LA ELABORACIÓN DE UN DOCUMENTO DE SEGURIDAD V 1.4

⁸ IBID



como la transmisión de datos y sus destinatarios, de acuerdo con las políticas internas que establezca la dependencia o entidad.

Procedimientos de control de acceso a la red que incluyan perfiles de usuarios o grupos de usuarios para el acceso restringido a las funciones y programas de los sistemas de los datos personales.

Deberán contar con mecanismos de auditoría o rastreabilidad de operaciones y así garantizar que el personal encargado del tratamiento de datos personales, sólo tenga acceso a las funciones autorizadas del sistema de datos personales según su perfil de usuario. Aplicar procedimientos de respaldo de base de datos y realizar pruebas periódicas de restauración, se tendrá que llevar el control de inventarios y clasificación de los medios magnéticos u ópticos de respaldo de los datos personales.

Utilizar un espacio externo seguro para guardar de manera sistemática los respaldos de base de datos personales y el transporte de los sistemas de datos personales, se debe de garantizar que, durante la transmisión de datos personales y el transporte de los soportes de almacenamiento, que no se pueda tener acceso a los datos, que no sean, reproducidos, alterados o suprimidos sin autorización.

La aplicación de los procedimientos para la destrucción de medios de almacenamiento y de respaldo obsoletos que contengan datos personales. En los casos en que la operación sea externa, convenir con el proveedor del servicio que la dependencia o entidad tenga la facultad de verificar que se respete la integridad, confiabilidad, confidencialidad y disponibilidad de los datos personales, revisar que el tratamiento se está realizando conforme a los contratos formalizados.

Diseñar planes de contingencia que garanticen la continuidad de la operación y realizar pruebas de eficiencia de los mismos.

Llevar a cabo las verificaciones a través de las áreas de tecnología de la información, informática o su equivalente y cualquier otra medida tendente a garantizar el cumplimiento de los principios de protección de datos personales.⁹

⁹ IBID



EDUCACIÓN

IDENTIFICACIÓN Y NIVELES DE SEGURIDAD POR UNIDAD ADMINISTRATIVA, A TRAVÉS DEL ORGANIGRAMA ESTRUCTURAL VIGENTE DE LA SECRETARÍA DE EDUCACIÓN DEL ESTADO DE JALISCO

15



EDUCACIÓN

Sistema de Protección de Información Confidencial por Área.

DESPACHO DE LA SECRETARÍA DE EDUCACIÓN		
DOCUMENTO	TIPO DE DOCUMENTO	NIVEL DE SEGURIDAD
AGENDA	FÍSICO Y ELECTRÓNICO	BÁSICO
QUEJAS	FÍSICO Y ELECTRÓNICO	ALTO
SOLICITUDES	FÍSICO Y ELECTRÓNICO	MEDIO

UNIDAD ADMINISTRATIVA	SECRETARÍA PARTICULAR
-----------------------	-----------------------

DOCUMENTO	TIPO DE DOCUMENTO	NIVEL DE SEGURIDAD
AGENDA	FÍSICO Y ELECTRÓNICO	BÁSICO

UNIDAD ADMINISTRATIVA	COORDINACIÓN GENERAL
-----------------------	----------------------

DOCUMENTO	TIPO DE DOCUMENTO	NIVEL DE SEGURIDAD
AGENDA	FÍSICO Y ELECTRÓNICO	BÁSICO

UNIDAD ADMINISTRATIVA:	COORDINADOR DE ASESORES
------------------------	-------------------------

DOCUMENTO	TIPO DE DOCUMENTO	NIVEL DE SEGURIDAD
QUEJAS	FÍSICO Y ELECTRÓNICO	ALTO
SOLICITUDES	FÍSICO Y ELECTRÓNICO	MEDIO



EDUCACIÓN

UNIDAD ADMINISTRATIVA:	DIRECCIÓN DE RELACIONES INTERNACIONALES
-------------------------------	--

DOCUMENTO	TIPO DE DOCUMENTO	NIVEL DE SEGURIDAD
EXPEDIENTES	FÍSICO	MEDIO
VIÁTICOS	FÍSICO	BÁSICO

UNIDAD ADMINISTRATIVA:	DIRECCIÓN DE COMUNICACIÓN SOCIAL, EDICIONES Y PUBLICACIONES
-------------------------------	--

DOCUMENTO	TIPO DE DOCUMENTO	NIVEL DE SEGURIDAD
No Aplica	No Aplica	No Aplica

UNIDAD ADMINISTRATIVA:	DIRECCIÓN GENERAL DE ATENCIÓN A LA COMUNIDAD EDUCATIVA
-------------------------------	---

DOCUMENTO	TIPO DE DOCUMENTO	NIVEL DE SEGURIDAD
QUEJAS	FÍSICO ELECTRONICO	BÁSICO
PETICIONES	FÍSICO ELECTRONICO	BÁSICO
GESTION	FÍSICO ELECTRÓNICO	BÁSICO



EDUCACIÓN

UNIDAD ADMINISTRATIVA:

UNIDAD DE TRANSPARENCIA E
INFORMACIÓN PÚBLICA DE LA
SECRETARÍA DE EDUCACIÓN.

DOCUMENTO	TIPO DE DOCUMENTO	NIVEL DE CONFIDENCIABILIDAD
SISTEMA INFOMEX (Nombre de solicitantes).	ELECTRÓNICO	BÁSICO
LIBRO DE REGISTROS DE SOLICITUDES DE INFORMACIÓN.	FÍSICO	BÁSICO
LIBRO DE REGISTRO DE OFICIOS (SALIENTES).	FÍSICO	BÁSICO
COPIA ELECTRÓNICA DE RESPUESTAS, AMPLIACIONES DE TÉRMINO, NOTIFICACIONES ITEI, PREVENCIÓNES, ASIGNACIONES.	ELECTRÓNICO	BÁSICO
EXPEDIENTES (Folios).	FÍSICO	MEDIO
BASE DE DATOS (Registro de Solicitudes de Información).	ELECTRÓNICO	BÁSICO



EDUCACIÓN

COMITÉ DE TRANSPARENCIA

DOCUMENTO	TIPO DE DOCUMENTO	NIVEL DE SEGURIDAD
SOLICITUDES DE DERECHOS ARCO	FÍSICO ELECTRÓNICO	ALTO
CLASIFICACIÓN DE INFORMACIÓN	FÍSICO ELECTRÓNICO	ALTO

UNIDAD ADMINISTRATIVA

COORDINACIÓN DE EDUCACIÓN BÁSICA

DOCUMENTO	TIPO DE DOCUMENTO	NIVEL DE SEGURIDAD
PETICIONES Y QUEJAS	FÍSICO Y ELECTRÓNICO	BÁSICO

UNIDAD ADMINISTRATIVA:

DIRECCIÓN GENERAL DE EDUCACIÓN PREESCOLAR

DOCUMENTO	TIPO DE DOCUMENTO	NIVEL DE SEGURIDAD
QUEJAS, ATENCIÓN Y SEGUIMIENTO	FÍSICO Y ELECTRÓNICO	BÁSICO
LISTADO DE CONTROL DE	FÍSICO	BÁSICO



EDUCACIÓN

ASISTENCIAS DEL PERSONAL ADSCRITO A ESTA DIRECCIÓN		
EXPEDIENTES DEL PERSONAL ADSCRITO A ESTA DIRECCIÓN	FÍSICO	MEDIO

UNIDAD ADMINISTRATIVA:	DIRECCIÓN DE GESTIÓN Y OPERACIÓN DE EDUCACIÓN PREESCOLAR
------------------------	--

DOCUMENTO	TIPO DE DOCUMENTO	NIVEL DE SEGURIDAD
No Aplica	No Aplica	No Aplica

UNIDAD ADMINISTRATIVA:	DIRECCIÓN DE PROYECTOS EDUCATIVOS DE EDUCACIÓN PREESCOLAR
------------------------	---

DOCUMENTO	TIPO DE DOCUMENTO	NIVEL DE SEGURIDAD
No Aplica	No Aplica	No Aplica



EDUCACIÓN

UNIDAD ADMINISTRATIVA:	DIRECCIÓN GENERAL DE EDUCACIÓN PRIMARIA
-------------------------------	--

DOCUMENTO	TIPO DE DOCUMENTO	NIVEL DE SEGURIDAD
QUEJAS, ATENCIÓN Y SEGUIMIENTO	FÍSICO Y ELECTRÓNICO	BÁSICO
LISTADO DE CONTROL DE ASISTENCIAS DEL PERSONAL ADSCRITO A ESTA DIRECCIÓN	FÍSICO	BÁSICO
EXPEDIENTES DEL PERSONAL ADSCRITO A ESTA DIRECCIÓN	FÍSICO	MEDIO

UNIDAD ADMINISTRATIVA:	DIRECCIÓN DE GESTIÓN Y OPERACIÓN DE EDUCACIÓN PRIMARIA
-------------------------------	---

DOCUMENTO	TIPO DE DOCUMENTO	NIVEL DE SEGURIDAD
No Aplica	No Aplica	No Aplica



EDUCACIÓN

UNIDAD ADMINISTRATIVA:	DIRECCIÓN DE PROYECTOS EDUCATIVOS DE EDUCACIÓN PRIMARIA
-------------------------------	--

DOCUMENTO	TIPO DE DOCUMENTO	NIVEL DE SEGURIDAD
No Aplica	No Aplica	No Aplica

UNIDAD ADMINISTRATIVA:	DIRECCIÓN GENERAL EDUCACIÓN SECUNDARIA
-------------------------------	---

DOCUMENTO	TIPO DE DOCUMENTO	NIVEL DE SEGURIDAD
QUEJAS, ATENCIÓN Y SEGUIMIENTO	FÍSICO Y ELECTRÓNICO	BÁSICO
EXPEDIENTES DEL PERSONAL ADSCRITO A ESTA DIRECCIÓN	FÍSICO	MEDIO

UNIDAD ADMINISTRATIVA:	DIRECCIÓN DE SECUNDARIA GENERAL
-------------------------------	--

DOCUMENTO	TIPO DE DOCUMENTO	NIVEL DE SEGURIDAD
QUEJAS, ATEMCIÓN Y SEGUIMIENTO	FÍSICO Y ELECTRONICO	BÁSICO



EDUCACIÓN

UNIDAD ADMINISTRATIVA:	DIRECCIÓN DE EDUCACIÓN SECUNDARIA TÉCNICA
-------------------------------	--

DOCUMENTO	TIPO DE DOCUMENTO	NIVEL DE SEGURIDAD
QUEJAS, ATEMCIÓN Y SEGUIMIENTO	FÍSICO Y ELECTRONICO	BÁSICO

UNIDAD ADMINISTRATIVA:	DIRECCIÓN DE EDUCACIÓN TELESECUNDARIA
-------------------------------	--

DOCUMENTO	TIPO DE DOCUMENTO	NIVEL DE SEGURIDAD
QUEJAS, ATEMCIÓN Y SEGUIMIENTO	FÍSICO Y ELECTRONICO	BÁSICO
PLANTILLA DE PERSONAL	ELECTRÓNICO	MEDIO
VISITAS DE SUPERVISIÓN	FISICO	BÁSICO
EXPEDIENTES DE SUPERVISORES	FISICO	MEDIO
MINUTARIO	FISICO	BÁSICO



EDUCACIÓN

UNIDAD ADMINISTRATIVA:	DIRECCIÓN GENERAL DE EDUCACIÓN PARA LA EQUIDAD Y FORMACIÓN INTEGRAL.
-------------------------------	---

DOCUMENTO	TIPO DE DOCUMENTO	NIVEL DE SEGURIDAD
ATENCIÓN Y SEGUIMIENTO DE SERVICIOS	FÍSICO Y ELECTRÓNICO	BÁSICO

UNIDAD ADMINISTRATIVA:	DIRECCIÓN DE EDUCACIÓN INICIAL
-------------------------------	---------------------------------------

DOCUMENTO	TIPO DE DOCUMENTO	NIVEL DE SEGURIDAD
EXPEDIENTES DE PERSONAL	FÍSICO	MEDIO
SOLICITUDES DE INSCRIPCIÓN	FÍSICO	MEDIO

UNIDAD ADMINISTRATIVA:	DIRECCIÓN DE EDUCACIÓN ESPECIAL
-------------------------------	--

DOCUMENTO	TIPO DE DOCUMENTO	NIVEL DE SEGURIDAD
SOLICITUD DE ATENCIÓN	FÍSICO	ALTO
	ELECTRÓNICO	ALTO



EDUCACIÓN

REGISTRO BASE DE DATOS		
ESTUDIO SOCIOECONOMICO	FÍSICO	ALTO
FICHA DE IDENTIFICACIÓN POR DISCAPACIDAD	FÍSICO	ALTO

UNIDAD ADMINISTRATIVA.	DIRECCIÓN DE EDUCACIÓN INDÍGENA
------------------------	---------------------------------

DOCUMENTO	TIPO DE DOCUMENTO	NIVEL DE SEGURIDAD
APOYO A PROBLEMÁTICAS DETECTADAS A ALUMNOS	EXPEDIENTE	ALTO

UNIDAD ADMINISTRATIVA:	DIRECCIÓN DE EDUCACIÓN FÍSICA Y DEPORTE
------------------------	---

DOCUMENTO	TIPO DE DOCUMENTO	NIVEL DE SEGURIDAD
No Aplica	No Aplica	No Aplica



EDUCACIÓN

UNIDAD ADMINISTRATIVA:	DIRECCIÓN DE PSICOPEDAGOGÍA
-------------------------------	------------------------------------

DOCUMENTO	TIPO DE DOCUMENTO	NIVEL DE SEGURIDAD
APOYO A DOCENTES Y ALUMNOS	FÍSICOS	ALTO

UNIDAD ADMINISTRATIVA:	DIRECCIÓN DE ARTICULACIÓN PARA LA EQUIDAD Y PREVENCIÓN DE LA VIOLENCIA
-------------------------------	---

DOCUMENTO	TIPO DE DOCUMENTO	NIVEL DE SEGURIDAD
No Aplica	No Aplica	No Aplica

UNIDAD ADMINISTRATIVA:	DIRECCIÓN GENERAL DE PROGRAMAS ESTRATÉGICOS
-------------------------------	--

DOCUMENTO	TIPO DE DOCUMENTO	NIVEL DE SEGURIDAD
No Aplica	No Aplica	No Aplica



EDUCACIÓN

UNIDAD ADMINISTRATIVA:	DIRECCIÓN DE PROGRAMAS DE TECNOLOGÍA EN EL AULA
-------------------------------	--

DOCUMENTO	TIPO DE DOCUMENTO	NIVEL DE SEGURIDAD
No Aplica	No Aplica	No Aplica

UNIDAD ADMINISTRATIVA:	DIRECCIÓN DE PROGRAMAS DE ACOMPAÑAMIENTO PEDAGÓGICO
-------------------------------	--

DOCUMENTO	TIPO DE DOCUMENTO	NIVEL DE SEGURIDAD
EXPEDIENTE DE PERSONAL	FÍSICO	ALTO

UNIDAD ADMINISTRATIVA:	DIRECCIÓN DE PROGRAMAS PARA EL DESARROLLO Y BIENESTAR ESCOLAR
-------------------------------	--

DOCUMENTO	TIPO DE DOCUMENTO	NIVEL DE CONFIDENCIALIDAD
LISTA DE DOTACIÓN DE ANTEOJOS	FÍSICO	ALTO
EXPEDIENTES DE CASOS ESPECIALES	FÍSICO	ALTO
EXPEDIENTES TÉCNICO DE ALUMNOS	ELECTRÓNICO	ALTO



EDUCACIÓN

UNIDAD ADMINISTRATIVA:	DIRECCIÓN DE PROGRAMAS COMPENSATORIOS Y DE APOYO
-------------------------------	---

DOCUMENTO	TIPO DE DOCUMENTO	NIVEL DE SEGURIDAD
PAGO COMPENSATORIO	FÍSICO Y ELECTRÓNICO	BÁSICO Y MEDIO

UNIDAD ADMINISTRATIVA:	DIRECCIÓN DE SEGUIMIENTO Y EVALUACIÓN DE LA GESTIÓN
-------------------------------	--

DOCUMENTO	TIPO DE DOCUMENTO	NIVEL DE SEGURIDAD
No Aplica	No Aplica	No Aplica

COORDINACIÓN:	COORDINACIÓN DE EDUCACIÓN MEDIA SUPERIOR
----------------------	---

DOCUMENTO	TIPO DE DOCUMENTO	NIVEL DE SEGURIDAD
ATENCIÓN A QUEJAS	FÍSICO Y ELECTRÓNICO	MEDIO
ATENCIÓN DE QUEJAS Y JUICIOS	FÍSICO	ALTO
GESTIÓN PRESUPUESTAL Y FINANCIERO	FÍSICO	BÁSICO



EDUCACIÓN

UNIDAD ADMINISTRATIVA:	DIRECCIÓN GENERAL DE EDUCACIÓN MEDIA SUPERIOR
-------------------------------	--

DOCUMENTO	TIPO DE DOCUMENTO	NIVEL DE SEGURIDAD
EXPEDIENTES DE PERSONAL	FÍSICO	ALTO

UNIDAD ADMINISTRATIVA:	DIRECCIÓN GENERAL DE ENLACE DE ORGANISMOS PÚBLICOS DESCENTRALIZADOS DE EDUCACIÓN MEDIA SUPERIOR
-------------------------------	--

DOCUMENTO	TIPO DE DOCUMENTO	NIVEL DE SEGURIDAD
EXPEDIENTES Y NOMBRAMIENTOS TITULARES OPD	FÍSICO	MEDIO
ATENCIÓN Y SEGUIMIENTO DE INFORMACIÓN DE ORGANISMOS.	FÍSICO Y ELECTRÓNICO	BÁSICO

UNIDAD ADMINISTRATIVA:	DIRECCIÓN ACADÉMICA DE EDUCACIÓN MEDIA SUPERIOR
-------------------------------	--

DOCUMENTO	TIPO DE DOCUMENTO	NIVEL DE SEGURIDAD
REGISTRO DE BASE DE DATOS	ELECTRÓNICO	BÁSICO
PLANTILLAS DE DOCENTES	ELECTRÓNICO	MEDIO
ATENCIÓN Y COORDINACIÓN DE PROGRAMAS	FISICO Y ELECTRONICO	BÁSICO



EDUCACIÓN

UNIDAD ADMINISTRATIVA:	DIRECCIÓN DE GESTIÓN ESTRATÉGICA DE EDUCACIÓN MEDIA SUPERIOR
-------------------------------	---

DOCUMENTO	TIPO DE DOCUMENTO	NIVEL DE SEGURIDAD
No Aplica	No Aplica	No Aplica

COORDINACIÓN	COORDINACIÓN DE FORMACIÓN Y ACTUALIZACIÓN DOCENTE, MAESTRIA EN EDUCACIÓN CON INTERVENCIÓN EN LA PRÁCTICA EDUCATIVA
---------------------	---

DOCUMENTO	TIPO DE DOCUMENTO	NIVEL DE SEGURIDAD
FORMACIÓN DE PROFESORES DE LA EDUCACIÓN	FÍSICO Y ELECTRÓNICO	MEDIO

UNIDAD ADMINISTRATIVA:	DIRECCIÓN GENERAL DE EDUCACIÓN NORMAL
-------------------------------	--

DOCUMENTO	TIPO DE DOCUMENTO	NIVEL DE SEGURIDAD
KARDEX	FÍSICO	ALTO
REGISTRO DE ESCOLARIDAD	FÍSICO	ALTO
CERTIFICADO DE ESTUDIOS	FÍSICO	ALTO

31



EDUCACIÓN

ACTAS DE EXAMEN PROFESIONAL	FÍSICO	ALTO
TÍTULOS	FÍSICO	ALTO
AUTORIZACIÓN PARA EJERCICIO DE DOCENCIA	FÍSICO	ALTO

UNIDAD ADMINISTRATIVA:	DIRECCIÓN DE GESTIÓN Y DESARROLLO INSTITUCIONAL
-------------------------------	--

DOCUMENTO	TIPO DE DOCUMENTO	NIVEL DE SEGURIDAD
No Aplica	No Aplica	No Aplica

UNIDAD ADMINISTRATIVA:	DIRECCIÓN GENERAL DE FORMACIÓN CONTINUA PARA PROFESIONALES DE LA EDUCACIÓN
-------------------------------	---

DOCUMENTO	TIPO DE DOCUMENTO	NIVEL DE SEGURIDAD
LISTADO DE DOCENTES	ELECTRÓNICO	MEDIO

UNIDAD ADMINISTRATIVA:	DIRECCIÓN DE DESARROLLO ACADÉMICO
-------------------------------	--

DOCUMENTO	TIPO DE DOCUMENTO	NIVEL DE SEGURIDAD
LISTADO DE DOCENTES	ELECTRÓNICO	MEDIO



EDUCACIÓN

UNIDAD ADMINISTRATIVA:	DIRECCIÓN DE GESTIÓN Y EVALUACIÓN DE PROFESIONALES DE LA EDUCACIÓN
-------------------------------	---

DOCUMENTO	TIPO DE DOCUMENTO	NIVEL DE SEGURIDAD
No Aplica	No Aplica	No Aplica

UNIDAD ADMINISTRATIVA:	DIRECCIÓN GENERAL DE UNIDADES DE UNIVERSIDAD PEDAGÓGICA NACIONAL E INSTITUCIONES DE POSGRADO
-------------------------------	---

DOCUMENTO	TIPO DE DOCUMENTO	NIVEL DE SEGURIDAD
PLANTILLA DOCENTE Y ADMINISTRATIVA.	ELECTRÓNICO Y FÍSICO	ALTO

UNIDAD ADMINISTRATIVA:	DIRECCIÓN UNIDADES DE LA UNIVERSIDAD PEDAGÓGICA NACIONAL
-------------------------------	---

DOCUMENTO	TIPO DE DOCUMENTO	NIVEL DE SEGURIDAD
EXPEDIENTES DE DOCENTES	FÍSICO	ALTO
INFORMACIÓN PERSONAL DE LOS ALUMNOS	ELECTRÓNICO Y FÍSICO	ALTO
ALUMNOS BECADOS, REPOSICIÓN Y ENTREGA DE TARJETAS	FÍSICO	ALTO



EDUCACIÓN

UNIDAD ADMINISTRATIVA:	DIRECCIÓN DE POSGRADO
-------------------------------	------------------------------

DOCUMENTO	TIPO DE DOCUMENTO	NIVEL DE SEGURIDAD
PROGRAMAS EDUCATIVOS DE POSGRADO PARTICULARES Y PÚBLICOS DICTAMINADOS; DE NUEVO INGRESO Y REESTRUCTURADOS	FÍSICO Y ELECTRÓNICO	ALTO
DICTAMINACIÓN DE PROTOCOLO DE TESIS QUE SOLICITAN BECA COMISIÓN	FÍSICO Y ELECTRÓNICO	ALTO
RELACIÓN DE CERTIFICADOS DE ESTUDIO Y ACTAS DE EXAMÉN PROFESIONAL	FÍSICO Y ELECTRÓNICO	ALTO

UNIDAD ADMINISTRATIVA:	DIRECCIÓN GENERAL EDUCACIÓN PERMANENTE
-------------------------------	---

DOCUMENTO	TIPO DE DOCUMENTO	NIVEL DE SEGURIDAD
EXPEDIENTES DE BECARIOS, ASESORES Y ALUMNOS	FÍSICO Y ELECTRÓNICOS	ALTO



EDUCACIÓN

UNIDAD ADMINISTRATIVA:	DIRECCIÓN DE CAPACITACIÓN PARA LA VIDA Y EL TRABAJO
-------------------------------	--

DOCUMENTO	TIPO DE DOCUMENTO	NIVEL DE SEGURIDAD
PLANEACIÓN DE MISIONES CULTURALES	FÍSICO	MEDIO
SERVICIO DE CAPACITACIÓN	FÍSICO	MEDIO
CERTIFICADO DE TERMINO	FÍSICO	ALTO
EXPEDIENTES DE ALUMNOS	FÍSICO	ALTO

UNIDAD ADMINISTRATIVA:	DIRECCIÓN DE ATENCIÓN AL REZAGO EDUCATIVO
-------------------------------	--

DOCUMENTO	TIPO DE DOCUMENTO	NIVEL DE CONFIDENCIALIDAD
REGISTRO Y CONTROL DE PERSONAL	FÍSICO	BÁSICO

COORDINACIÓN:	COORDINACIÓN DE PLANEACIÓN Y EVALUACIÓN EDUCATIVA
----------------------	--

DOCUMENTO	TIPO DE DOCUMENTO	NIVEL DE SEGURIDAD
No Aplica	No Aplica	No Aplica



EDUCACIÓN

UNIDAD ADMINISTRATIVA:	DIRECCIÓN GENERAL DE PLANEACIÓN EDUCATIVA
-------------------------------	--

DOCUMENTO	TIPO DE DOCUMENTO	NIVEL DE SEGURIDAD
No Aplica	No Aplica	No Aplica

UNIDAD ADMINISTRATIVA:	DIRECCIÓN DE ESTADÍSTICA Y SISTEMAS DE INFORMACIÓN
-------------------------------	---

DOCUMENTO	TIPO DE DOCUMENTO	NIVEL DE SEGURIDAD
EXPEDIENTES DE PERSONAL ADSCRITO A LA DIRECCIÓN	FÍSICO	BÁSICO
CONSULT@ME (consultas)	ELECTRÓNICO	BÁSICO
SISTEMAS DE PAGOS (SIAPSEP-SIAN)	ELECTRÓNICO	BÁSICO
GESTIÓN EDUCATIVA	ELECTRÓNICO	BÁSICO



EDUCACIÓN

UNIDAD ADMINISTRATIVA	DIRECCIÓN DE PROGRAMACIÓN Y PRESUPUESTO
------------------------------	--

DOCUMENTO	TIPO DE DOCUMENTO	NIVEL DE SEGURIDAD
No Aplica	No Aplica	No Aplica

UNIDAD ADMINISTRATIVA	DIRECCIÓN DE ATENCIÓN A LA INFRAESTRUCTURA ESCOLAR
------------------------------	---

DOCUMENTO	TIPO DE DOCUMENTO	NIVEL DE SEGURIDAD
No Aplica	No Aplica	No Aplica

UNIDAD ADMINISTRATIVA	DIRECCIÓN DE BECAS
------------------------------	---------------------------

DOCUMENTO	TIPO DE DOCUMENTO	NIVEL DE SEGURIDAD
OTORGAMIENTO DE BECAS	FÍSICO Y ELECTRÓNICO	ALTO
EXPEDIENTES DE SOLICITUDES DE BECAS	FÍSICO Y ELECTRÓNICO	ALTO
BASES DE DATOS DE BECARIOS Y EX BECARIOS	FÍSICO Y ELECTRÓNICO	ALTO

37



EDUCACIÓN

UNIDAD ADMINISTRATIVA	DIRECCIÓN GENERAL DE EVALUACIÓN EDUCATIVA
------------------------------	--

DOCUMENTO	TIPO DE DOCUMENTO	NIVEL DE SEGURIDAD
APLICACIÓN DE EVALUACIONES EDUCATIVAS	FÍSICOS Y ELECTRÓNICOS	ALTO

UNIDAD ADMINISTRATIVA	DIRECCIÓN DE EVALUACIÓN PARA EL FORTALECIMIENTO EDUCATIVO
------------------------------	--

DOCUMENTO	TIPO DE DOCUMENTO	NIVEL DE SEGURIDAD
No Aplica	No Aplica	No Aplica

UNIDAD ADMINISTRATIVA	DIRECCIÓN DE EVALUACIÓN DEL SISTEMA EDUCATIVO ESTATAL
------------------------------	--

DOCUMENTO	TIPO DE DOCUMENTO	NIVEL DE SEGURIDAD
No Aplica	No Aplica	No Aplica

Handwritten signature in blue ink.

Handwritten mark in blue ink, possibly initials.

Handwritten mark in blue ink, possibly a signature or initials.



EDUCACIÓN

UNIDAD ADMINISTRATIVA:	DIRECCIÓN GENERAL DE ACREDITACIÓN, INCORPORACIÓN Y REVALIDADCIÓN EDUCATIVA
-------------------------------	---

DOCUMENTO	TIPO DE DOCUMENTO	NIVEL DE SEGURIDAD
SISTEMA AUTOMATIZADO DE LA ADMINISTRACIÓN DE ACREDITACIÓN, INCORPORACIÓN Y REVALIDADCIÓN EDUCATIVA	FÍSICO Y ELECTRÓNICO	ALTO

UNIDAD ADMINISTRATIVA	DIRECCIÓN DE CONTROL ESCOLAR DE EDUCACIÓN BÁSICA
------------------------------	---

DOCUMENTO	TIPO DE DOCUMENTO	NIVEL DE SEGURIDAD
SISTEMA AUTOMATIZADO DE LA ADMINISTRACIÓN DE CONTROL ESCOLAR	FÍSICO Y ELECTRÓNICO	ALTO



EDUCACIÓN

UNIDAD ADMINISTRATIVA	DIRECCIÓN DE CONTROL ESCOLAR DE EDUCACIÓN MEDIA SUPERIOR Y EDUCACIÓN SUPERIOR DOCENTE
------------------------------	--

DOCUMENTO	TIPO DE DOCUMENTO	NIVEL DE SEGURIDAD
SISTEMA AUTOMATIZADO DE LA ADMINISTRACIÓN DE CONTROL ESCOLAR	FÍSICO Y ELECTRÓNICO	ALTO

UNIDAD ADMINISTRATIVA	DIRECCIÓN DE INCORPORACIÓN, REVALIDACIÓN Y EQUIVALENCIAS
------------------------------	---

DOCUMENTO	TIPO DE DOCUMENTO	NIVEL DE SEGURIDAD
No Aplica	No Aplica	No Aplica

UNIDAD ADMINISTRATIVA:	DIRECCIÓN DE PARTICIPACIÓN SOCIAL
-------------------------------	--

DOCUMENTO	TIPO DE DOCUMENTO	NIVEL DE SEGURIDAD
TODOS LOS REGISTROS DE CONSEJOS ESCOLARES	FÍSICO Y ELECTRÓNICO	BÁSICO



EDUCACIÓN

COORDINACIÓN:	COORDINACIÓN DE ADMINTRACIÓN
----------------------	-------------------------------------

DOCUMENTO	TIPO DE DOCUMENTO	NIVEL DE SEGURIDAD
No Aplica	No Aplica	No Aplica

UNIDAD ADMINISTRATIVA:	DIRECCIÓN GENERAL DE PERSONAL
-------------------------------	--------------------------------------

DOCUMENTO	TIPO DE DOCUMENTO	NIVEL DE SEGURIDAD
SIAPSEP	ELECTRONICO	ALTO
CONSULTAME	ELECTRONICO	ALTO
NÓMINA	FÍSICO	BÁSICO
PENSIÓN ALIMENTICIA	FÍSICO	ALTO
EXPEDIENTES LABORALES	FÍSICO	ALTO
EXPEDIENTES JURÍDICOS	FÍSICO	ALTO

Handwritten signature

Handwritten mark

Handwritten signature



EDUCACIÓN

UNIDAD ADMINISTRATIVA:	DIRECCIÓN DE GESTIÓN Y CONTROL DE PERSONAL
-------------------------------	---

DOCUMENTO	TIPO DE DOCUMENTO	NIVEL DE SEGURIDAD
EXPEDIENTES LABORALES	FÍSICO	ALTO
COORDINACIÓN Y EVALUACIÓN PARA LA ADMINISTRACIÓN DE PERSONAL	FÍSICO Y ELECTRÓNICO	ALTO

UNIDAD ADMINISTRATIVA:	DIRECCIÓN DE PLANEACIÓN Y DE RECURSOS HUMANOS
-------------------------------	--

DOCUMENTO	TIPO DE DOCUMENTO	NIVEL DE SEGURIDAD
COORDINACIÓN Y EVALUACIÓN PARA LA ADMINISTRACIÓN DE PERSONAL	FÍSICO Y ELECTRÓNICO	ALTO
REGISTRO BASE DE DATOS	ELECTRÓNICO	ALTO

UNIDAD ADMINISTRATIVA:	DIRECCIÓN DE ADMINISTRACIÓN DE PERSONAL
-------------------------------	--

DOCUMENTO	TIPO DE DOCUMENTO	NIVEL DE SEGURIDAD
COORDINACIÓN Y EVALUACIÓN	FÍSICO Y ELECTRÓNICO	ALTO



EDUCACIÓN

PARA LA ADMINISTRACIÓN DE PERSONAL		
REGISTRO BASE DE DATOS	ELECTRÓNICO	ALTO

UNIDAD ADMINISTRATIVA:	DIRECCIÓN DE CAPACITACIÓN Y DESARROLLO
-------------------------------	---

DOCUMENTO	TIPO DE DOCUMENTO	NIVEL DE SEGURIDAD
COORDINACIÓN Y EVALUACIÓN PARA LA ADMINISTRACIÓN DE PERSONAL	FÍSICO Y ELECTRÓNICO	ALTO

UNIDAD ADMINISTRATIVA:	DIRECCIÓN DE RELACIONES LABORALES
-------------------------------	--

DOCUMENTO	TIPO DE DOCUMENTO	NIVEL DE SEGURIDAD
COORDINACIÓN Y EVALUACIÓN PARA LA ADMINISTRACIÓN DE PERSONAL	FÍSICO Y ELECTRÓNICO	ALTO
EXPEDIENTES LABORALES	FÍSICO	ALTO
EXPEDIENTES JURÍDICOS	FÍSICO	ALTO



EDUCACIÓN

UNIDAD ADMINISTRATIVA: DIRECCIÓN DE REMUNERACIONES

DOCUMENTO	TIPO DE DOCUMENTO	NIVEL DE SEGURIDAD
COORDINACIÓN Y EVALUACIÓN PARA LA ADMINISTRACIÓN DE PERSONAL	FÍSICO Y ELECTRÓNICO	ALTO

UNIDAD ADMINISTRATIVA: DIRECCIÓN GENERAL DE RECURSOS MATERIALES Y SERVICIOS GENERALES

DOCUMENTO	TIPO DE DOCUMENTO	NIVEL DE SEGURIDAD
No Aplica	No Aplica	No Aplica

UNIDAD ADMINISTRATIVA: DIRECCIÓN DE CONTROL DE BIENES MUEBLES E INMUEBLES

DOCUMENTO	TIPO DE DOCUMENTO	NIVEL DE SEGURIDAD
No Aplica	No Aplica	No Aplica

UNIDAD ADMINISTRATIVA: DIRECCIÓN DE SERVICIOS GENERALES

DOCUMENTO	TIPO DE DOCUMENTO	NIVEL DE SEGURIDAD
No Aplica	No Aplica	No Aplica



EDUCACIÓN

UNIDAD ADMINISTRATIVA:	DIRECCIÓN DE ADQUISICIONES
-------------------------------	-----------------------------------

DOCUMENTO	TIPO DE DOCUMENTO	NIVEL DE SEGURIDAD
No Aplica	No Aplica	No Aplica

UNIDAD ADMINISTRATIVA:	DIRECCIÓN GENERAL CONTABILIDAD Y RECURSOS FINANCIEROS
-------------------------------	--

DOCUMENTO	TIPO DE DOCUMENTO	NIVEL DE SEGURIDAD
SOLICITUD DE PAGO ANTE SEFIN	FÍSICO	BÁSICO
CHEQUERAS Y GASTOS DE OPERACIÓN	FÍSICO	MEDIO
PAGO DE TRANSFERENCIAS ELECTRONICAS, INVERSIÓN	ELECTRÓNICO	ALTO
COPIA DE TARJETAS DE FIRMAS DE CUENTAS DE CHEQUES	FÍSICO	ALTO
FACTURAS	FÍSICO	BÁSICO

UNIDAD ADMINISTRATIVA:	DIRECCIÓN DE CONTABILIDAD
-------------------------------	----------------------------------

DOCUMENTO	TIPO DE DOCUMENTO	NIVEL DE SEGURIDAD
ADMINISTRACIÓN Y CONTROL DE	FÍSICO Y ELECTRÓNICO	ALTO

[Handwritten signature]

[Handwritten signature]

[Handwritten signature]



EDUCACIÓN

RECURSOS FINANCIEROS		
----------------------	--	--

UNIDAD ADMINISTRATIVA:	DIRECCIÓN INGRESOS Y EGRESOS
------------------------	------------------------------

DOCUMENTO	TIPO DE DOCUMENTO	NIVEL DE SEGURIDAD
ADMINISTRACIÓN Y CONTROL DE RECURSOS FINANCIEROS	FÍSICO Y ELECTRÓNICO	ALTO

UNIDAD ADMINISTRATIVA:	DIRECCIÓN GENERAL DE TECNOLOGÍAS DE LA INFORMACIÓN.
------------------------	---

DOCUMENTO	TIPO DE DOCUMENTO	NIVEL DE SEGURIDAD
TECNOLOGÍA INSTITUCIONAL	FÍSICO Y ELECTRÓNICO	ALTO

UNIDAD ADMINISTRATIVA:	DIRECCIÓN DE MANTENIMIENTO A LA INFRAESTRUCTURA TECNOLÓGICA EN LAS ESCUELAS
------------------------	---

DOCUMENTO	TIPO DE DOCUMENTO	NIVEL DE SEGURIDAD
NO APLICA	NO APLICA	NO APLICA

Handwritten signature in blue ink.

Handwritten signature in blue ink.

Handwritten signature in blue ink.



EDUCACIÓN

UNIDAD ADMINISTRATIVA:	DIRECCIÓN DE CENTROS DE ATENCIÓN Y SERVICIOS
-------------------------------	---

DOCUMENTO	TIPO DE DOCUMENTO	NIVEL DE SEGURIDAD
REGISTRO DE COMISIONES ESCOLARES DE LOS CENTROS DE ATENCIÓN Y SERVICIOS	FÍSICOS Y ELECTRÓNICOS	MEDIO

UNIDAD ADMINISTRATIVA:	DIRECCIÓN DE COORDINACIÓN DE CARRERA MAGISTERIAL
-------------------------------	---

DOCUMENTO	TIPO DE DOCUMENTO	NIVEL DE SEGURIDAD
ESTIMULOS PARA PROFESORES DE EDUCACIÓN BÁSICA	FÍSICOS Y ELECTRÓNICOS	MEDIO

UNIDAD ADMINISTRATIVA:	DIRECCIÓN OPERATIVA DEL CENTRO DE CAPACITACIÓN
-------------------------------	---

DOCUMENTO	TIPO DE DOCUMENTO	NIVEL DE SEGURIDAD
NO APLICA	NO APLICA	NO APLICA

Handwritten signature in blue ink.

Handwritten mark in blue ink, resembling a stylized 'X' or signature.

Handwritten signature in blue ink.



EDUCACIÓN

UNIDAD ADMINISTRATIVA:	DIRECCIÓN DE ORGANIZACIÓN Y NORMATIVIDAD
-------------------------------	---

DOCUMENTO	TIPO DE DOCUMENTO	NIVEL DE SEGURIDAD
NO APLICA	NO APLICA	NO APLICA

UNIDAD ADMINISTRATIVA:	UNIDAD MEDICO-ODONTOLOGICA
-------------------------------	-----------------------------------

DOCUMENTO	TIPO DE DOCUMENTO	NIVEL DE SEGURIDAD
LICENCIA MÉDICA	FÍSICO	ALTO
EXPEDIENTE CLÍNICO DE PACIENTES	FÍSICO	ALTO
HOJA DIARIA DEL MEDICO	FÍSICO	ALTO
PASE DE SALIDA DEL PACIENTE	FÍSICO	ALTO
CONSTANCIA DE ASISTENCIA A CONSULTA A DIFERENTES CLÍNICAS	FÍSICO	ALTO

COORDINACIÓN:	COORDINACIÓN DELEGACIONES REGIONALES
----------------------	---

DOCUMENTO	TIPO DE DOCUMENTO	NIVEL DE SEGURIDAD
NO APLICA	NO APLICA	NO APLICA



EDUCACIÓN

UNIDAD ADMINISTRATIVA:	DIRECCIÓN GENERAL DE SERVICIOS EDUCATIVOS REGIONALES
-------------------------------	---

DOCUMENTO	TIPO DE DOCUMENTO	NIVEL DE SEGURIDAD
NO APLICA	NO APLICA	NO APLICA

UNIDAD ADMINISTRATIVA:	DRSE NORTE, ALTOS NORTE, ALTOS SUR, CIÉNEGA, SURESTESUR, SIERRA DE AMULA, COSTA SUR, COSTA NORTE, SIERRA OCCIDENTAL, VALLES, CENTRO 1, CENTRO 2, CENTRO 3.
-------------------------------	---

DOCUMENTO	TIPO DE DOCUMENTO	NIVEL DE SEGURIDAD
PREINSCRIPCIONES, INSCRIPCIONES Y REINSCRIPCIONES	FÍSICO Y ELECTRONICO	ALTO
NOMINAS	FÍSICO Y ELECTRONICO	ALTO
LAUDOS EMITIDOS POR DIFERENTES INSTANCIAS JUDICIALES	FÍSICO	ALTO

UNIDAD ADMINISTRATIVA:	DIRECCIÓN GENERAL DE ASUNTOS JURÍDICOS
-------------------------------	---

DOCUMENTO	TIPO DE DOCUMENTO	NIVEL DE SEGURIDAD
SUSTANCIACIÓN, DESAHOGO E INSTAURACIÓN DE PROCEDIMIENTOS	FÍSICOS	ALTO



EDUCACIÓN

EXPEDIENTES DEL PERSONAL QUE LABORA EN LA DIRECCIÓN GENERAL	FÍSICO	ALTO
EXPEDIENTES DE LOS INMUEBLES DE LA SEJ	FÍSICO	ALTO
PROCEDIMIENTOS DE INFRACCIÓN ADMINISTRATIVA	FÍSICO	ALTO
PROCEDIMIENTOS DE RESPONSABILIDAD ADMINISTRATIVA	FÍSICO	ALTO
PROCEDIMIENTOS ADMINISTRATIVOS	FÍSICO	ALTO
COPIA DE LOS JUICIOS QUE SE VENTILAN EN CONTRA DE LA SEJ	FÍSICO	ALTO
EXPEDIENTES DE CONVENIOS QUE CELEBRA LA SEJ	FÍSICO	MEDIO
EXPEDIENTES DE PETICIONES DIVERSAS	FÍSICO	MEDIO

UNIDAD ADMINISTRATIVA: DIRECCIÓN DE INMUEBLES

DOCUMENTO	TIPO DE DOCUMENTO	NIVEL DE SEGURIDAD
NO APLICA	NO APLICA	NO APLICA



EDUCACIÓN

UNIDAD ADMINISTRATIVA:	DIRECCIÓN DE LO ADMINISTRATIVO, LABORAL E INFRACCIONES ADMINISTRATIVAS
-------------------------------	---

DOCUMENTO	TIPO DE DOCUEMNTO	NIVEL DE SEGURIDAD
SUSTANCIACIÓN, DESAHOGO E INSTAURACIÓN DE PROCEDIMIENTOS	FÍSICOS	ALTO

UNIDAD ADMINISTRATIVA:	DIRECCIÓN DE LO CONTENCIOSO
-------------------------------	------------------------------------

DOCUMENTO	TIPO DE DOCUEMNTO	NIVEL DE SEGURIDAD
SUSTANCIACIÓN, DESAHOGO E INSTAURACIÓN DE PROCEDIMIENTOS	FÍSICOS	ALTO

UNIDAD ADMINISTRATIVA:	DIRECCIÓN DE LO CONSULTIVO
-------------------------------	-----------------------------------

DOCUMENTO	TIPO DE DOCUEMNTO	NIVEL DE SEGURIDAD
SUSTANCIACIÓN, DESAHOGO E INSTAURACIÓN DE PROCEDIMIENTOS	FÍSICOS	ALTO



EDUCACIÓN

UNIDAD ADMINISTRATIVA:	DIRECCIÓN GENERAL DE LA CONTRALORÍA
-------------------------------	--

DOCUMENTO	TIPO DE DOCUMENTO	NIVEL DE SEGURIDAD
AUDITORIAS A UNIDADES ADMINISTRATIVAS, PLANTELES Y ÓRGANOS	FÍSICO Y ELECTRÓNICO	BÁSICO
ACTA ENTREGA-RECEPCIÓN DE LAS UNIDADES ADMINISTRATIVAS	FÍSICO Y ELECTRÓNICO	BÁSICO
PADRÓN DE OBLIGADOS A PRESENTAR DECLARACIÓN DE SITUACIÓN PATRIMONIAL PARA CONTRALORÍA DEL ESTADO	ELECTRÓNICO	MEDIO
NOTIFICACIÓN DE CONTRALORÍA DEL ESTADO A ESTA DEPENDENCIA DE LOS SERVIDORES PÚBLICOS ADSCRITOS A ESTA SECRETARÍA QUE ESTÁN OMISOS EN LA PRESENTACIÓN DE SU DECLARACIÓN DE SITUACIÓN PATRIMONIAL CORRESPONDIENTE.	FÍSICO	MEDIO
AMONESTACIÓN POR ESCRITO A SERVIDORES PÚBLICOS ADSCRITOS A ESTA	FÍSICO	MEDIO



EDUCACIÓN

SECRETARÍA, POR PRESENTAR SU DECLARACIÓN DE SITUACIÓN PATRIMONIAL CORRESPONDIENTE DE FORMA EXTEMPORANEA EN CONTRALORÍA DEL ESTADO		
ATENCIÓN DE QUEJAS	FÍSICO Y ELECTRÓNICO	BÁSICO
EXPEDIENTES	FÍSICO	MEDIO
ACTAS CIRCUNSTANCIADAS	FÍSICO Y ELECTRÓNICO	BÁSICO
RESOLUTIVO DE EXPEDIENTES	FÍSICO	MEDIO

UNIDAD ADMINISTRATIVA:	DIRECCIÓN DE AUDITORIA
-------------------------------	-------------------------------

DOCUMENTO	TIPO DE DOCUMENTO	NIVEL DE SEGURIDAD
AUDITORIAS A UNIDADES ADMINISTRATIVAS, PLANTELES Y ÓRGANOS	FÍSICO Y ELECTRÓNICO	ALTO

UNIDAD ADMINISTRATIVA:	DIRECCIÓN DE CONTROL Y SEGUIMIENTO
-------------------------------	---

DOCUMENTO	TIPO DE DOCUMENTO	NIVEL DE SEGURIDAD
SEGUIMIENTO A AUDITORIAS A UNIDADES ADMINISTRATIVAS, PLANTELES Y ÓRGANOS	FÍSICO Y ELECTRÓNICO	ALTO



DE LAS SANCIONES

Del mal uso o prácticas que se lleven en contra del presente y de lo mencionado por la legislación vigente, devienen responsabilidades que puede ser de carácter penal, administrativa o civil.

A continuación, se transcriben las medidas de apremio y las sanciones devenidas de diversas infracciones a la norma.

De conformidad a la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios, se contará con las siguientes medidas de apremio y responsabilidades respecto de los Datos que pose esta Secretaría.

“Artículo 139. Medidas de apremio.

1. El Instituto podrá interponer las siguientes medidas de apremio para asegurar el cumplimiento de las determinaciones emitidas:

I. Amonestación pública;

II. Multa equivalente a la cantidad de ciento cincuenta hasta mil quinientas veces el valor diario de la Unidad de Medida y Actualización; o

III. Arresto administrativo.

2. El incumplimiento de los Responsables, será difundido en los portales de obligaciones de transparencia del Instituto y considerado en las evaluaciones que realice.

3. En caso de que el incumplimiento de las determinaciones del Instituto implique la presunta comisión de un delito, se deberán denunciar los hechos ante la autoridad competente.

4. Las medidas de apremio de carácter económico no podrán ser cubiertas con recursos públicos.

Artículo 140. Medidas de apremio — Incumplimiento.

1. Si a pesar de la ejecución de las medidas de apremio previstas en el artículo anterior, no se cumple la resolución del Instituto, se requerirá el cumplimiento al superior jerárquico para que en el plazo de cinco días obligue a cumplir sin demora.

2. De persistir el incumplimiento se aplicarán sobre el superior jerárquico las medidas de apremio establecidas en el artículo anterior.

3. Transcurrido el plazo, sin que se haya dado cumplimiento, se dará vista a la autoridad competente en materia de responsabilidades.



Artículo 141. Medidas de apremio — Determinación.

I. Para calificar las medidas de apremio establecidas en el presente Capítulo, el Instituto deberá considerar:

I. La gravedad de la falta del responsable, determinada por elementos tales como el daño causado; los indicios de intencionalidad; la duración del incumplimiento de las determinaciones del Instituto y la afectación al ejercicio de sus atribuciones;

II. La condición económica del infractor; y

III. La reincidencia.

2. El Instituto establecerá mediante lineamientos de carácter general, las atribuciones de las áreas encargadas de calificar la gravedad de la falta de observancia de sus determinaciones y de la notificación y ejecución de las medidas de apremio que apliquen e implementen, conforme a los elementos desarrollados en el presente Capítulo.

3. El Instituto podrá requerir al infractor la información necesaria para determinar su condición económica, apercibido de que en caso de no proporcionar la misma, las multas se cuantificarán con base en los elementos que se tenga a disposición, entendidos como los que se encuentren en los registros públicos, los que contengan medios de información o sus propias páginas de internet y, en general, cualquiera que evidencie su condición, quedando facultado el Instituto para requerir aquella documentación que se considere indispensable para tal efecto a las autoridades competentes.

Artículo 142. Medidas de apremio — Ejecución.

1. Las medidas de apremio deberán aplicarse e implementarse en un plazo máximo de quince días, contados a partir de que sea notificada la medida de apremio al infractor.

Artículo 143. Medidas de apremio — Reincidencia.

1. Se considerará reincidente al que habiendo incurrido en una infracción que haya sido sancionada, cometa otra del mismo tipo o naturaleza.

2. En caso de reincidencia, el Instituto podrán imponer una multa hasta el doble de la que se hubiera determinado la primera vez.

Artículo 144. Multas — Naturaleza.

1. Las multas que fije el Instituto se harán efectivas, impuestas como sanciones administrativas de acuerdo con esta Ley; constituyen créditos fiscales a favor del Estado y su ejecución se rige por las disposiciones jurídicas aplicables.

Artículo 145. Amonestación Pública — Naturaleza.

1. Las amonestaciones públicas serán impuestas por el Instituto y será ejecutada por el superior jerárquico inmediato del infractor con el que se relacione.



EDUCACIÓN

Capítulo II Infracciones y Sanciones

Artículo 146. Infracciones— Causales.

1. Serán causas de responsabilidad y sanción por incumplimiento de las obligaciones establecidas en la materia de la presente Ley, las siguientes:

I. Actuar con negligencia, dolo o mala fe durante la sustanciación de las solicitudes para el ejercicio de los derechos ARCO o de la portabilidad de los datos personales;

II. Incumplir los plazos de atención previstos en la presente Ley para responder las solicitudes para el ejercicio de los derechos ARCO o para hacer efectivo el derecho de que se trate;

III. Ampliar con dolo los plazos previstos en la presente Ley para responder las solicitudes para el ejercicio de los derechos ARCO o la portabilidad de los datos personales;

IV. Usar, sustraer, divulgar, ocultar, alterar, mutilar, destruir o inutilizar, total o parcialmente y de manera indebida datos personales, que se encuentren bajo su custodia o a los cuales tengan acceso o conocimiento con motivo de su empleo, cargo o comisión;

V. Dar tratamiento, de manera intencional, a los datos personales en contravención a los principios y deberes establecidos en la presente Ley;

VI. Mantener los datos personales inexactos cuando resulte imputable al responsable;

VII. No efectuar la rectificación, cancelación u oposición al tratamiento de los datos personales que legalmente proceda, cuando resulten afectados los derechos de los titulares;

VIII. No contar con el aviso de privacidad, o bien, omitir en el mismo alguno de los elementos a que refieren los artículos 21, 22 y 23 de la presente Ley, según sea el caso, y demás disposiciones aplicables;

IX. Clasificar, con dolo o negligencia, datos personales sin que se cumplan las características señaladas en Ley de Transparencia. La sanción sólo procederá cuando exista una resolución previa, que haya quedado firme, respecto del criterio de clasificación de los datos personales;

X. Incumplir el deber de confidencialidad establecido en el artículo 44 de la presente Ley;

XI. No establecer las medidas de seguridad en los términos que establecen los artículos 30, 31, 32, 33, 34, 35 y 36 de la presente Ley;

XII. Presentar vulneraciones a los datos personales por la falta de implementación de medidas de seguridad según los artículos 30, 31, 37, 42 y 43 de la presente Ley;



XIII. Llevar a cabo la transferencia de datos personales, en contravención a lo previsto en la presente Ley;

XIV. Obstruir los actos de verificación de la autoridad;

XV. Crear bases de datos personales en contravención a lo dispuesto por la presente Ley;

XVI. No acatar las resoluciones emitidas por el Instituto;

XVII. Aplicar medidas compensatorias en contravención de los criterios que tales fines establezca el Sistema Nacional;

XVIII. Declarar dolosamente la inexistencia de datos personales cuando éstos existan total o parcialmente en los archivos del responsable;

XIX. No atender las medidas cautelares establecidas por el Instituto;

XX. Tratar los datos personales de manera que afecte o impida el ejercicio de los derechos fundamentales previstos en la Constitución Política de los Estados Unidos Mexicanos;

XXI. No cumplir con las disposiciones previstas en los artículos 65, 66, 68 y 69, de la presente Ley;

XXII. No presentar ante el Instituto la evaluación de impacto a la protección de datos personales en aquellos casos en que resulte obligatoria, de conformidad con lo previsto en la presente Ley y demás normativa aplicable;

XXIII. Realizar actos para intimidar o inhibir a los titulares en el ejercicio de los derechos ARCO; y

XXIV. Omitir la entrega del informe anual a que se refiere el artículo 44, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública, o bien, de manera extemporánea.

2. Las causas de responsabilidad previstas en las fracciones I, IV, V, IX, XII, XIII, XIV, XVI, XVIII, XX y XXI, así como la reincidencia en las conductas previstas en el resto de las fracciones de este artículo, serán consideradas como graves para efectos de su sanción administrativa.

3. Las sanciones de carácter económico no podrán ser cubiertas con recursos públicos.

Artículo 147. Infracciones— De partidos políticos.

1. Ante incumplimientos por parte de los partidos políticos, el Instituto dará vista, según corresponda, al Instituto Nacional Electoral o al Instituto Electoral y de Participación Ciudadana del Estado de Jalisco, para que investigue, resuelva y, en su caso, sancione la conducta, sin perjuicio de las sanciones establecidas para los partidos políticos en las leyes aplicables.



Artículo 148. Infracciones— De fideicomisos o fondos públicos.

1. En el caso de probables infracciones relacionadas con fideicomisos o fondos públicos, el Instituto deberá dar vista al órgano interno de control o instancia equivalente del responsable relacionado con éstos, cuando sean servidores públicos, con el fin de que instrumenten los procedimientos administrativos a que haya lugar.

Artículo 149. Infracciones— Sanciones.

1. A quien cometa alguna de las infracciones establecidas en la presente Ley, se le sancionará de la siguiente forma:

I. El apercibimiento para que el Responsable lleve a cabo los actos solicitados por el titular, en los términos previstos por esta Ley, tratándose de los supuestos previstos en el artículo 146, en sus fracciones II, VI, XIV, XVII, XIX y XXIV del artículo anterior;

II. Multa de ciento cincuenta a quinientas veces el valor diario de la Unidad de Medida y Actualización, en los casos previstos en el artículo 146, en sus fracciones III, V, VII, VIII, XI, XV, XIII, XXI, XXII y XXIII; y

III. Multa de quinientas a mil quinientas veces el valor diario de la Unidad de Medida y Actualización, en los casos previstos en el artículo 146, en sus fracciones I, IV, IX, X, XII, XVI, XVIII, XX y XXI.

Artículo 150. Infracciones — Determinación.

1. El Instituto fundará y motivará la determinación de las infracciones y sanciones, considerando:

I. La naturaleza del dato;

II. La notoria improcedencia de la negativa del responsable, para realizar los actos solicitados por el titular, en términos de esta Ley;

III. El carácter intencional o no, de la acción u omisión constitutiva de la infracción;

IV. La capacidad económica del Responsable; y

V. La reincidencia.

Artículo 151. Infracciones— Responsabilidad Administrativa.

1. Independientemente de la sanción que aplique el Instituto, éste deberá presentar ante las autoridades competentes denuncia en materia de responsabilidad administrativa de los servidores públicos para que, de ser procedente, se sancione al servidor público de conformidad con la Ley de Responsabilidades de los Servidores Públicos del Estado de Jalisco. En el caso de que se imponga como sanción la inhabilitación.

Artículo 152. Infracciones— Procedencia de responsabilidades del orden civil o penal.



1. Las responsabilidades que resulten de los procedimientos administrativos correspondientes, derivados de la violación a lo dispuesto por el artículo 177 de la presente Ley, son independientes de las del orden civil, penal o de cualquier otro tipo que se puedan derivar de los mismos hechos.

2. Dichas responsabilidades se determinarán, en forma autónoma, a través de los procedimientos previstos en las leyes aplicables y las sanciones que, en su caso, se impongan por las autoridades competentes, también se ejecutarán de manera independiente.

3. Para tales efectos, el Instituto podrá denunciar ante las autoridades competentes cualquier acto u omisión violatoria de la presente Ley y aportar las pruebas que consideren pertinentes, en los términos de las leyes aplicables.

CÓDIGO CIVIL DEL ESTADO DE JALISCO

"Artículo 1394¹⁰ que a la letra dice:

Cuando el daño moral haya afectado a la víctima en su decoro, honor, prestigio personal o profesional, el juez independientemente de lo dispuesto en el artículo anterior ordenará y en ejecución de sentencia a petición expresa del afectado y con cargo al responsable, la publicación de un extracto de la sentencia de la que se desprenda con toda claridad las circunstancias y el alcance de la misma a través de los medios informativos que considere convenientes; pero en los casos en que el daño se produzca por medio de un acto que haya sido difundido por los medios informativos o de difusión masiva, el juez ordenará que los mismos den publicidad al extracto de la sentencia con la misma importancia y consideración que hubiere tenido la difusión original.

Artículo 1394 BIS¹¹.-

Estarán sujetas a la reparación del daño moral de acuerdo a lo establecido en el artículo anterior y por tanto, se considerarán como hechos ilícitos, las siguientes conductas:

- I. *El que divulgue la imputación que se hace a otra persona física o jurídica, de un hecho falso o cierto, determinado o indeterminado, que pueda causarle deshora, descrédito perjuicio o exponerlo al desprecio de alguien.*

¹⁰ SANCIONES ESTABLECIDAS EN EL CÓDIGO CIVIL

¹¹ IBID



- II. *El que impute a otro un hecho determinado y calificado como delito por la ley, si el hecho es falso o inocente la persona a quien se le imputa.*
- III. *El que presente denuncias o querellas calumniosas, entendiéndose por tales aquellas en que su autor imputa un delito a persona determinada, sabiendo que ésta es inocente o aquél no se ha cometido.*
- IV. *Al que ofenda el honor, ataque a la vida privada o la imagen de la propia persona.*

La reproducción fiel de información no da lugar al daño moral, aun en los casos en que la información reproducida no sea correcta y pueda dañar el honor de alguna persona pues no constituye una responsabilidad para el que difunde dicha información siempre y cuando se cite la fuente de donde se obtuvo.¹²

CÓDIGO PENAL DEL ESTADO DE JALISCO

El Código Penal consagra en el caso de revelación de secretos y en el espionaje, se considera agravada la responsabilidad cuando dichos actos se cometen por funcionarios o empleados públicos (arts. 129-211)¹³

Delitos cometidos en la custodia o guarda de documentos artículo 151¹⁴.-

Se impondrán de uno a cuatro años de prisión a los servidores públicos que indebidamente:

- I. *Substraigan, destruyan u oculten documentos, papeles u objetos que les hayan sido confiados, o a los que tengan acceso por razón de su cargo.*

¹² Fraga, Gabino Derecho Administrativo, Editorial Porrúa S.A. pág. 140-141

¹³ CÓDIGO PENAL (ARTÍCULOS 129-211)

¹⁴ CÓDIGO PENAL DEL ESTADO DE JALISCO



- II. Quebranten o consientan en quebrantar los sellos de documentos o efectos sellados por autoridad competente que tengan bajo su custodia; y
- III. Abran, o consientan que se abran sin la autorización correspondiente, papeles o documentos cerrados que tengan bajo su custodia.

REGLAMENTOS

REGLAMENTO DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA GUBERNAMENTAL

Artículo 5.- Las dependencias y entidades podrán establecer mecanismos de colaboración entre sí o con el Instituto para cumplir con las obligaciones establecidas en la Ley, este Reglamento y los lineamientos expedidos por este último, particularmente en lo que se refiere a las obligaciones de transparencia, a los procedimientos de acceso a la información, a los datos personales y a la corrección de éstos, así como al establecimiento y operación de las Unidades de Enlace y los Comités.¹⁵

Protección de datos personales contemplados en el citado Reglamento

Artículo 47. Los procedimientos para acceder a los datos personales que estén en posesión de las dependencias y entidades garantizarán la protección de los derechos de los individuos, en particular, a la vida privada y a la intimidad, así como al acceso y corrección de sus datos personales, de conformidad con los lineamientos que expida el Instituto y demás disposiciones aplicables para el manejo, mantenimiento, seguridad y protección de los datos personales.¹⁶

Artículo 48. Las dependencias y entidades que cuenten con sistemas de datos personales deberán hacer del conocimiento del Instituto y del público en general a través de sus sitios de internet, el listado de dichos sistemas, en el cual indicarán el objeto del sistema, el tipo de datos que contiene, el uso que se les da, la unidad

¹⁵ REGLAMENTO DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA GUBERNAMENTAL.

¹⁶ IBID



administrativa que lo administra y el nombre del responsable. El Instituto mantendrá un listado público actualizado de los sistemas de datos personales que sean hechos de su conocimiento.¹⁷

GLOSARIO

Para efectos de la aplicación de las presentes Recomendaciones, además de las definiciones contenidas en el artículo 3º de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental publicada en el Diario Oficial de la Federación el 11 de junio 2002, en el artículo 2 de su reglamento, publicado en el mismo Diario el 11 junio de 2003, y en el Lineamiento tercero de los Lineamientos de Protección de Datos Personales expedidos por el Instituto y publicados en el Diario Oficial de la FEDERACIÓN EL 30 de septiembre de 2005, se entenderá por:

- Área de consulta de datos personales: El espacio destinado para que el personal autorizado examine aquellos datos personales que están autorizados a consultar, sin posibilidad de modificar su contenido.
- Área de recepción de datos personales: El espacio donde se reciben datos personales en cualquier tipo de soporte (físico, electrónico, o ambos) en tanto se siguen las demás fases de su tratamiento para integrarlos a uno o más.
- Área de resguardo de datos personales: El espacio para almacenar datos personales que han recibido el tratamiento correspondiente para que formen parte integral de uno o más datos personales, sin importar el soporte (físico, electrónico, o ambos) en tanto se siguen las demás fases de su tratamiento para integrarlos a uno o más datos personales.
- Destinatario: Cualquier persona física o moral o privada que reciba datos personales.
- Divulgación de incidentes: Las acciones que adoptan el Titular de la dependencia o entidad y el Responsable de los datos personales, a

¹⁷ IBID



efecto de dar a conocer a las autoridades competentes, a los titulares de los datos y, en su caso, al público en general, los actos deliberados (intrusión, robo, etc.), los acontecimientos de caso fortuito o de fuerza mayor (desastres naturales, incendios, huelgas, etc.), que hubieran ocasionado pérdida total o parcial de los datos personales bajo su custodia.

- Encargado: El servidor público o cualquier otra persona física o moral facultado por un instrumento jurídico o expresamente autorizado por el Responsable para llevar a cabo el tratamiento físico o automatizado de los datos personales.
- Intrusión: Acción que una o más personas realizan para introducirse, sin derecho, en uno o más datos personales a fin de alterar, copiar o sustraer datos que forman parte de esos sistemas.
- Malware: Software malicioso o maligno utilizado por personas para causar daños en una o más computadoras o para sustraer archivos de los equipos; es decir, virus, gusanos cibernéticos, caballos de Troya, "spyware", "bots", "rootkits", y los que se creen posteriormente con el mismo propósito.
- Manual de operaciones: Conjunto de documentos que enumeran, definen y detallan los procesos y procedimientos que los servidores públicos llevan a cabo dentro de una dependencia o entidad.
- Obsolescencia: Mal desempeño comparado a las nuevas tecnologías, imposibilidad de encontrar repuestos adecuados, nuevas tecnologías que reemplazan la antigua (tecnologías sustantivas), dos o más tecnologías salidas en una época determinada y que compiten entre sí, pero donde una termina superando a las otras.



- Personal autorizado: Los usuarios o encargados (servidores públicos) que han recibido autorización para interactuar con uno o más datos personales por parte del Responsable del sistema.
- Personal de sistemas: El personal que labora en el área de tecnologías de información, sistemas, telecomunicaciones.
- Responsable: 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.
- Sistema "Persona": Aplicación informática desarrollada por el Instituto para mantener actualizado el listado de los sistemas de datos personales que posean las dependencias y entidades para registrar e informar sobre las transmisiones, modificaciones y cancelaciones de los mismos.
- Sistema de datos personales: Constituye el conjunto ordenado de datos personales que estén en posesión de una dependencia o entidad, con independencia de su forma de acceso, creación, almacenamiento u organización.

Los sistemas de datos personales podrán distinguirse entre físicos y automatizados, definiéndose cada uno de ellos de la siguiente forma:

Físicos.- Conjunto ordenado de datos que para su tratamiento están contenidos en registros manuales, impresos, sonoros, magnéticos, visuales u holográficos.

Automatizados: Conjunto ordenado de datos que para su tratamiento han sido o están sujetos a un tratamiento informático y que por ende requieren de una herramienta tecnológica específica para su acceso, recuperación o tratamiento.



- Soportes electrónicos: Medios de almacenamiento inteligibles sólo mediante el uso de algún aparato con circuitos que procese su contenido para examinar, modificar o almacenar los datos; es decir, cintas magnéticas de audio, vídeo y datos, fichas de microfilm, discos ópticos (CD Y DVD).
- Soportes Físicos: Medios de almacenamiento inteligibles a simple vista, es decir, que no requieren de ningún aparato que procese su contenido para examinar, modificar o almacenar los datos, es decir, formularios impresos llenados "a mano" o "máquina", fotografías y placas radiológicas, entre otros.
- Supervisión interna: Proceso sistemático mediante el cual se realiza la recopilación, acumulación y evaluación de evidencia sobre la adopción y práctica de las medidas de seguridad recomendadas en este documento por una dependencia o entidad. Sus propósitos son precisar e informar el grado de cumplimiento entre la información recabada y los criterios establecidos.
- Titular de los datos: Persona física a quien se refieren los datos personales que sean objeto de tratamiento.
- Transmisión: Toda entrega total o parcial de sistemas de datos personales realizada por las dependencias y entidades a cualquier persona distinta al Titular de los datos, mediante el uso de medios físicos o electrónicos tales como la interconexión de base 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.



- Tratamiento: Operaciones y procedimientos físicos o automatizados que permitan recabar, registrar, reproducir, conservar, organizar, modificar, transmitir y cancelar datos personales.
- Usuario: Servidor Público facultado por un instrumento jurídico o expresamente autorizado por el Responsable que utiliza de manera cotidiana datos personales para el ejercicio de sus atribuciones, por lo que accede a los sistemas de datos personales, sin posibilidad de agregar o modificar su contenido.
- Zona de acceso restringido: Todas aquellas áreas a las que sólo tienen acceso el personal autorizado y el personal de vigilancia; es decir, el área de recepción, el área de resguardo y el área de consulta de datos personales.

ANEXO 1.

Para un mejor funcionamiento del documento de Seguridad de Datos Personales, deberá contener¹⁸:

(Nombre de la Coordinación) (Denominación de la Unidad Administrativa)

Responsable:

- Nombre:
- Cargo:
- Funciones: (Descripción de las atribuciones con relación al tratamiento de los datos personales)
- Obligaciones: (Descripción de las responsabilidades en cuanto al tratamiento de Datos Personales)

Encargados:

- Nombre: (Nombre del Encargado 1)
- Cargo:
- Funciones:

¹⁸ GUÍA PARA LA ELABORACIÓN DEL DOCUMENTO DE SEGURIDAD V 1.4



EDUCACIÓN

- Obligaciones:
- Nombre: (Nombre del Encargado 2)
- Cargo:
- Funciones:
- Obligaciones:

Usuarios:

- Nombre: (Nombre del Usuario 1)
- Cargo:
- Funciones:
- Obligaciones:
- Nombre: (Nombre del Usuario 2)
- Cargo:
- Funciones:
- Obligaciones:

Así mismo un Folio de registro de cada uno de los datos recabados.

(Nombre del Sistema Persona)

Responsible:

- Nombre:
- Cargo:
- Funciones.
- Obligaciones:

Encargados:

- Nombre: (Nombre del Encargado 1)
- Cargo:
- Funciones:
- Obligaciones:
- Nombre: (Nombre del encargado2)
- Cargo:



- Funciones
- Obligaciones:

Usuarios:

- Nombre: (Nombre del Usuario)
 - Cargo:
 - Funciones:
 - Obligaciones:
-
- Nombre: (Nombre del Usuario)
 - Cargo:
 - Funciones:
 - Obligaciones:

Ejemplo:

Datos de Identificación (nombres, apellido paterno, apellido materno, domicilio, estado civil)

Datos laborales (correo electrónico institucional y teléfono institucional)

ANEXO 2.

ORIENTACIÓN DE LA ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE DATOS PERSONALES¹⁹

(Nombre del Sistema)

1. Tipo de soporte: (En caso de que se prevea cambiar el tipo de soporte que utiliza ejemplo, de físico a electrónico en el supuesto de que se prevea utilizar ambos tipos de soportes.)
 - a) Tipo de soporte: Precisar si el sistema se encuentra en soportes
 - b) Descripción: (Describir el soporte en el que se encuentran los datos físicos podrían ser en formatos, listados, documentos o expedientes,

¹⁹ GUIA PARA LA ELABORACIÓN DE UN DOCUMENTO DE SEGURIDAD V 1.4



entre otros y para soportes electrónicos, hoja de cálculo o base de datos relacional entre otros.

2. Característica del lugar donde guardan los soportes:
(Describir el lugar en el que físicamente se encuentran los soportes del sistema)

ORIENTACIÓN DE TRANSMISIÓN DE SOPORTES FÍSICOS DE DATOS PERSONALES

- Mensajero Oficial
- Asistente Secretarial
- Visita personal
- Servicio de Mensajería Externo
- El paquete con Datos Personales viaja en sobre cerrado, debidamente sellado, de tal forma que sea perceptible cualquier violación o apertura no autorizada del mismo.
- Sólo deberá entregarse si el destinatario acredita su identidad. Para ello el destinatario presenta una identificación oficial con fotografía y el mensajero reciba nombre, firma y un número de referencia que aparezca en tal identificación, además de la fecha de entrega.
- Si el destinatario no puede acreditar su identidad, el mensajero devuelve el paquete al transmisor.
- El transmisor deberá verificar que si fue entregado el paquete al destinatario si el paquete fue entregado a otra persona, da inicio de atención de un incidente.
- Se registra en la bitácora.
- Solo podrá ser enviado en correspondencia ordinaria si los datos personales requieren de un nivel de protección básico.
- El encargado es quien anota lo siguiente: Quien solicita el acceso, cuando se lleva a cabo (fecha y hora de entrada y salida), la razón que lo motiva y número del expediente utilizado.



ORIENTACIÓN DE TRANSMISIÓN DE SOPORTES ELECTRÓNICOS DE DATOS PERSONALES

- Las bitácoras de eventos ocurridos en sistemas electrónicos deberán llevar un estricto control y registro de:

Eventos ocurridos en equipos operativos (servidores, cortafuegos, almacenamiento masivo) que habilitan la operación del sistema de datos personales, así como intentos de acceso (exitosos y fallidos), accesos denegados a usuarios y terminales; uso de herramientas para administración del servidor y fecha y hora de los eventos anteriores.

- Cuando son eventos a nivel de software aplicativo del sistema de datos personales, deberán generarse bitácoras para mensajes de error, apertura, modificación y cierre de archivos, violaciones detectadas por el software aplicativo, fecha y hora de estos eventos.
- Si los eventos son relativos a las actividades de usuarios (capturistas, encargados, el propio responsable y el administrador del servidor) en interacción con el sistema deberán generar bitácoras para archivos, servicios y recursos utilizados, intentos de acceso (exitoso y fallidos); comandos y operaciones iniciadas, fecha y hora de los eventos.

REQUISITOS PARA LA ELABORACIÓN DE BITÁCORAS

- Quién accede a los datos personales
- Desde donde y con qué
- Accesos (intentos exitosos y fallidos) y salidas
- Propósito del acceso (sólo para modificaciones en el software aplicativo)
- Operaciones llevadas a cabo de datos personales (registros y campos) utilizados de la base de datos, fecha y hora.
- Cada semana se llevará a cabo un análisis de bitácoras pero no de todas ellas, solo de las que cuenten con mayor amenaza detectada. Además de lo establecido en las Medidas de Seguridad a Nivel Federal.



REQUISITOS PARA LA ELABORACIÓN DE INCIDENTES

- El Encargado elabora y entrega un informe al Responsable a más tardar al día siguiente de haber ocurrido el incidente, en el cual precisa los soportes físicos o electrónicos afectados y si fueron recuperados.
- Se deberá registrar en una hoja de cálculo anotando quien resolvió el incidente y los soportes dañados y recuperados, esta hoja deberá estar protegida con una contraseña de acceso. Además de las contempladas en las Medidas de Seguridad a nivel Federal.



EDUCACIÓN

**APROBACIÓN DEL DOCUMENTO DE SEGURIDAD
RESPONSABLE DEL DESARROLLO:**

Nombre: Lic. Isaura de Jesús Ortega Larios

Cargo: Directora Operativa de la Unidad de Transparencia

Teléfono: 38192717 ext. 22523

Correo electrónico: isaura.ortega@jalisco.gob.mx

REVISÓ:

Nombre: Dr. Rogelio Ríos González

Cargo: Secretario del Comité de Transparencia

Teléfono: 38192773

Correo electrónico: rogelio.rios@jalisco.gob.mx

AUTORIZÓ:

Nombre: Lic. María Yesenia Galván Beltrán

Cargo: Presidenta en Delegación del Comité de Transparencia

Teléfono: 30307500 ext. 53700

Correo electrónico: yesenia.galvan@jalisco.gob.mx

Nombre: Dr. Rogelio Ríos González

Cargo: Secretario del Comité de Transparencia

Teléfono: 38192773

Correo electrónico: rogelio.rios@jalisco.gob.mx

Nombre: Lic. Carlos Felipe Estrada Gutiérrez

Cargo: Integrante del Comité de Transparencia

Teléfono: 30307500 ext. 53631

Correo electrónico: carlos.gutierrez@jalisco.gob.mx



EDUCACIÓN

ATENTAMENTE

Guadalajara, Jal., a 15 de agosto de 2018

**"2018, Centenario de la Creación del municipio de Puerto Vallarta y del
XXX Aniversario del Nuevo Hospital Civil de Guadalajara"**

Lic. María Yesenia Galván Beltrán

Presidenta en Delegación del Comité de Transparencia

Dr. Rogelio Ríos González
Secretario del Comité de Transparencia

Lic. Carlos Felipe Estrada Gutiérrez
Integrante del Comité de Transparencia

La presente hoja de firmas corresponde al Documento de seguridad, aprobado por el Comité de Transparencia de la Secretaría de Educación del Estado de Jalisco, el día 15 de agosto de 2018.

ljo/RRG