COMITÉ DE TRANSPARENCIA DEL CONSEJO ESTATAL PARA LA PREVENCION DEL SINDROME DE INMUNODEFICIENCIA ADQUIRIDA EN JALISCO (COESIDA).

En Zapopan, Jalisco, siendo las 13:00 horas del día 15 de diciembre de 2019, en las instalaciones donde se ubica el Consejo Estatal para la Prevención del Síndrome de Inmunodeficiencia Adquirida (COESIDA), en la Calle Lago Tequesquitengo No. 2600, en la Colonia Lagos del Country, en Zapopan, Jalisco; estando presente los integrantes del Comité de Transparencia del Consejo Estatal para la Prevención del Síndrome de Inmunodeficiencia Adquirida e invitados el DR. LUIS ALBERTO RUIZ MORA, SECRETARIO TÉCNICO DEL COESIDA, Y PRESIDENTE DE ESTE COMITÉ, LA LIC. LIBNA LIZANIA VILLEGAS ROMERO, EN FUNCIÓN DE REPRESENTANTE DEL ORGANO INTERNO DE CONTROL DE LA SECRETARIA DE SALUD JALISCO, C. SORHAYA CAROLINA SALAZAR ARROYO, APOYO ADMINISTRATIVO EN SALUD A6, TITULAR DE LA UNIDAD DE TRANSPARENCIA, Y SECRETARIO DE ESTE COMITÉ DE TRANSPARENCIA DEL COESIDA, ACUERDAN LA REALIZACION DE LA TERCERA REUNIÓN DEL COMITÉ DE ACUERDO A LA PRESENTE ACTA BAJO EL SIGUIENTE:

ORDEN DEL DIA

1.- LISTA DE PRESENTES

2.- ACTUALIZACIÓN Y ABROBACIÓN DE LOS AVISOS DE PRIVACIDAD CORTO, SIMPLIFICADO E INTEGRAL, DE PRIVACIDAD FOCALIZADO EN LA COORDINACIÓN DE ADMINISTRACIÓN Y CONTABILIDAD, AVISO DE VIDEO VIGILANCIA, ELABORACIÓN, APROBACIÓN Y PUBLICACIÓN DE DOCUMENTO DE SEGURIDAD

3.- CIERRE DEL ACTA

DESAHOGO DE LA ORDEN DEL DIA

PRIMER PUNTO:

En el desahogo del primer punto de la orden del día se hace constar por parte del Presidente del Comité, la asistencia de los integrantes del Comité de Transparencia DR. LUIS ALBERTO RUIZ MORA, Presidente, LIC. LIBNA LIZANIA VILLEGAS ROMERO, quien funge como representante del Órgano Interno de Control de la SSJ, Y, LA C. SORHAYA CAROLINA SALAZAR ARROYO, Secretario del Comité, por lo que se toma constancia de que se encuentra la totalidad de los integrantes del comité y se pasa la lista correspondiente.

Declarándose el Quórum legal establecido para su realización.

SEGUNDO PUNTO:

En el Desahogo del Segundo punto de la orden del día el Secretario del comité y titular de la unidad de transparencia solicita el uso de la voz, para manifestar lo siguiente: De acuerdo a expedición y aprobación por parte del Congreso del Estado de la Ley de Protección de Datos Personales en Posesión de Sujetos

Obligados del Estado de Jalisco y sus Municipios, para el cumplimiento en lo dispuesto en su Transitorio Séptimo que señala: Los sujetos obligados responsables expedirán sus avisos de privacidad en los términos previstos en la presente Ley y demás disposiciones aplicables.

Por tal motivo es necesario que este comité de transparencia instruya al secretario para la actualización de los avisos de privacidad en los términos que establece la ley antes mencionada.

En uso de la voz de los integrante del comité acuerdan dar instrucciones al secretario para la actualización y elaboración de los avisos de privacidad y publicación del documento de seguridad.

En tal sentido previo un receso que se otorgó para la elaboración de los citados avisos el Secretario de este Comité de Trasparencia pone en consideración del pleno las propuestas de los avisos corto, simplificado, integral, focalizado y video vigilancia, así como el documento de seguridad, mismo que una vez revisados, discutidos y corregidos quedan de acuerdo a los documentos que se anexan a la siguiente acta.

Siendo estos:

1.- AVISO DE PRIVACIDAD CORTO, ANEXO 1

2.- AVISO SIMPLIFICADO, ANEXO 2

3.- AVISO INTEGRAL, ANEXO 3

4.- AVISO FOCALIZADO, ANEXO 4

5.- AVISO VIDEO VIGILANCIA, ANEXO 5

6.- DOCUMENTO DE SEGURIDAD

Se somete a aprobación los avisos de privacidad y documento de seguridad presentados a este comité, tomándose el siguiente acuerdo: Se aprueban los avisos de privacidad, corto, simplificado, integral, focalizado y video vigilancia, así como el documento de seguridad en los términos de la Ley de Protección de Datos Personales en posesión de Sujetos Obligados, otorgando los asistentes su aprobación en forma unánime.

Se faculta al Secretario para que realice los trámites necesarios para que dichos avisos y documento de seguridad en los que así corresponda se los compartan con el área de comunicación social de este sujeto obligado para la publicación correspondiente en la página Web, al Titular de la Unidad de Transparencia para su publicación en el Portal de Transparencia Estatal y Nacional, así como a las áreas que manejan datos personales e información confidencial para que compartan el aviso con sus usuarios de los servicios públicos que se ofrecen.

TERCER PUNTO:

En el desahogo del tercer punto de la orden del día se da por cerrada y concluida la presente acta del Comité de Transparencia, acordándose su aprobación por unanimidad todos los puntos ahí mencionados a las 17:00 horas del día 15 de diciembre de 2019, firmando los que en ella intervinieron pudieron y quisieron hacerlo.

COMITÉ DE TRANSPARENCIA DEL CONSEJO ESTATAL PARA LA PREVENCION DEL SINDROME DE INMUNODEFICIENCIA ADQUIRIDA

DR. LUIS ALBERTO RUIZ MORA
PRESIDENTE DEL COMITÉ DE TRANSPARENCIA DE COESIDA
SECRETARIO TECNICO DEL COESIDA

C. SORHAYA CAROLINA SALAZAR ARROYO
SECRETARIO DEL COMITÉ DE TRANSPARENCIA DE COESIDA
TITULAR UNIDAD DE TRANSPARENCIA

LIC. LIBNA LIZANIA VILLEGAS ROMERO
REPRESENTANTE ORGANO INTERNO DE CONTROL

COESIDA
Consejo Estatal para la Prevención del SIDA

Jalisco
GOBIERNO DEL ESTADO

AVISO DE PRIVACIDAD CORTO

En términos de lo que establece la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios el Consejo Estatal para la Prevención del Sida (COESIDA), con domicilio en Lago Tequesquitengo # 2600, Col Lagos del Country, C.P. 45177, Zapopan, Jalisco; es responsable del tratamiento de datos personales que se recaben con la finalidad de llevar a cabo la integración de una base de datos y control de expedientes para nuestras funciones, obligaciones y atribuciones.

Para mayor información sobre el uso de sus datos personales, puede consultar nuestro aviso de privacidad integral en https://transparencia.info.jalisco.gob.mx/sites/default/files/AVISO%20DE%20PRIVACIDAD%20COESIDA.pdf

AVISO DE PRIVACIDAD SIMPLIFICADO DEL CONSEJO ESTATAL PARA LA PREVENCION DEL SINDROME DE INMUNODEFICIENCIA ADQUIRIDA (COESIDA)

El Consejo Estatal para la Prevención del Síndrome de Inmunodeficiencia Adquirida en lo siguiente COESIDA, ubicado en Calle Lago Tequesquitengo #2600, colonia Lagos del Country, C.P.45177 en Zapopan, Jalisco, es el responsable del uso y protección de sus datos personales, y al respecto le informa lo siguiente:

Los datos personales que usted proporcione al COESIDA JALISCO, podrán ser recabados directa o indirectamente en medios electrónicos, por escrito y/o vía telefónica, serán utilizados exclusivamente para llevar a cabo los objetivos y atribuciones de este Consejo, serán única y exclusivamente utilizados para llevar a cabo los objetivos y atribuciones de este Consejo siempre bajo su consentimiento informado y los utilizaremos para las siguientes finalidades: Detección oportuna, canalización a los servicios de atención integral de las personas positivas a VIH, para una atención pronta y de calidad; para la correcta administración de medicamentos antirretrovirales a los pacientes y protección de sus datos personales en la base de datos llamada Sistema de Administración, Logística y Vigilancia de Antiretrovirales (SALVAR), así como las bases de datos derivadas de dicho sistema. La seguridad y resguardo de la información, así como para la integridad del personal y pacientes mediante el sistema de video vigilancia interno de COESIDA, la tramitación de solicitudes de información y ejercicio de derechos ARCO (Acceso, Rectificación, Cancelación y Oposición), trámites y asuntos administrativos, el registro de los participantes, ponentes e invitados a los eventos y capacitaciones que promueve el COESIDA, dar trámite a denuncias y/o quejas interpuestas en contra de los servidores públicos del COESIDA, garantizar la validez de los procedimientos que realiza el Comité de Transparencia, contar con los datos identificativos y documentación legal de las personas físicas que fungen como proveedores de bienes y servicios y la celebración de convenios con personas físicas y/o jurídicas.

Con relación a la transferencia de los datos personales, se informa que en los casos previstos por el artículo 22 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios, no se requiere la autorización del titular de la información confidencial para proporcionar a terceros.

Es importante señalar que sus datos personales son considerados información confidencial, por lo que se informa que no se realizaran transferencias de datos personales, con excepción de cualquier información que permita transparentar las acciones y garantizar el derecho a la información pública, aquella que obre en fuentes de acceso público, en virtud de que constituye información susceptible de ser publicada y difundida, de conformidad con lo establecido por la Ley en comento; o se esté en alguno de los supuestos descritos en los artículos 15 y 75 de la Ley de Protección de Datos Personales en Posesión de Sujetos

Obligados del Estado de Jalisco y sus municipios.

Usted puede solicitar ante este Sujeto Obligado, en cualquier tiempo, su Acceso, Rectificación, Cancelación, Oposición o Revocación del consentimiento, mediante la presentación de solicitud de ejercicios de derechos ARCO ante la Unidad de Transparencia del COESIDA, en Calle Lago Tesquitengo #2600, colonia Lagos del Country, C.P. 45177 en Zapopan, Jalisco.

Para mayor información sobre el uso de sus datos personales, puede consultar nuestro aviso de privacidad integral en:

https://transparencia.info.jalisco.gob.mx/sites/default/files/AVISO%20DE%20PRIVACIDAD%20COESIDA.pdf

15 de diciembre del 2019

AVISO DE PRIVACIDAD DEL CONSEJO ESTATAL PARA LA PREVENCION DEL SINDROME DE INMUNODEFICIENCIA ADQUIRIDA (COESIDA)

Versión Integral

El Consejo Estatal para la Prevención del Síndrome de Inmunodeficiencia Adquirida en lo siguiente COESIDA, ubicado en Calle Lago Tequesquitengo #2600, colonia Lagos del Country, C.P.45177 en Zapopan, Jalisco, es el responsable del uso y protección de sus datos personales, y al respecto le informa lo siguiente:

La protección de sus datos personales se realiza de conformidad a lo establecido en el artículo 6, Apartado A, fracción IV de la Constitución Política de los Estados Unidos Mexicanos, en los artículos 4 y 9 fracciones II, V y VI de la Constitución Política del Estado de Jalisco, en el artículo 29 fracción III y 35 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios y en el artículo 3. 1. Fracciones III, XXXII, 10, 19.2, 24, 87.1 fracciones I y X, y 90 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados Del Estado de Jalisco y sus Municipios.

El tratamiento de sus datos personales se realiza de conformidad a lo establecido en las atribuciones dentro del Reglamento Interno de este Consejo en los artículos 7 y 8, Capitulo 1, artículo 10, Capitulo II del Presidente, articulo 11, 12, 13, 14 y 15 del Capítulo III del Consejo de Vocales, articulo 26 y 27 del Capítulo IV del Coordinador, articulo 28, 29, 30, 31 y 32 del Capítulo V del Secretario Técnico, articulo 33, 37, 39, 41, 44, 45, 46, 47 y 49 del Capítulo VI de las Coordinaciones.

Los datos personales sensibles, se refieren a aquellos que requieren de especial protección como son: datos relacionados a la salud, ideológicos, de origen étnico o conlleve un riesgo grave para éste; Los datos personales se refieren a la información concerniente a una persona física identificada o identificable.

Los datos personales que serán sometidos a tratamiento son:

Datos Sensibles	**Datos Personales**
Huella digital Tipo de sangre Preferencia sexual Datos de salud	Nombre Domicilio Teléfono Sexo Edad Grado máximo de estudios Correo electrónico Firma Peso Talla Clave de Elector Imagen Corporal Registro Federal de Contribuyentes (RFC) Clave Única de Registro de Población (CURP) Fecha de Nacimiento Numero de Póliza del Sistema de Protección Social en Salud (Seguro Popular) Numero de Seguridad Social (IMSS, ISSSTE) Referencia Familiar (nombre y teléfono)

Dichos datos podrán ser recabados, directa o indirectamente, por medios electrónicos, por escrito y por teléfono, los datos personales que usted proporcione al COESIDA, serán única y exclusivamente utilizados para llevar a cabo los objetivos y atribuciones de este Consejo siempre bajo su consentimiento informado y los utilizaremos para las siguientes finalidades: Detección oportuna, canalización a los servicios de atención integral de las personas positivas a VIH, para una atención pronta y de calidad; para la correcta administración de medicamentos antirretrovirales a los pacientes y protección de sus datos personales en la base de datos llamada Sistema de Administración, Logística y Vigilancia de Antiretrovirales (SALVAR), así como las bases de datos derivadas de dicho sistema. La seguridad y resguardo de la información, así como para la integridad del personal y pacientes mediante el sistema de video vigilancia interno de COESIDA, la tramitación de solicitudes de información y ejercicio de derechos ARCO (Acceso, Rectificación, Cancelación y Oposición), trámites y asuntos administrativos, el registro de los

participantes, ponentes e invitados a los eventos y capacitaciones que promueve el COESIDA, dar trámite a denuncias y/o quejas interpuestas en contra de los servidores públicos del COESIDA, garantizar la validez de los procedimientos que realiza el Comité de Transparencia, contar con los datos identificativos y documentación legal de las personas físicas que fungen como proveedores de bienes y servicios y la celebración de convenios con personas físicas y/o jurídicas.

Es importante señalar que sus datos personales son considerados información confidencial, por lo que se informa que no se realizaran transferencias de datos personales, con excepción de cualquier información que permita transparentar las acciones y garantizar el derecho a la información pública, aquella que obre en fuentes de acceso público, en virtud de que constituye información susceptible de ser publicada y difundida, de conformidad con lo establecido por la Ley en comento; o se esté en alguno de los supuestos descritos en los artículos 15 y 75 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus municipios.

Se le informa que no se consideran transferencias las remisiones, ni la comunicación de datos entre áreas o Unidades Administrativas adscritas al mismo sujeto obligado en el ejercicio de sus atribuciones.

Usted puede solicitar ante el Consejo Estatal para la Prevención del Sida (COESIDA), en cualquier tiempo, su Acceso, Rectificación, Cancelación, Oposición o Revocación del consentimiento, mediantelapresentacióndesolicituddeejerciciodederechosARCOanteLa Unidad de Transparencia del COESIDA o bien ante la Plataforma Nacional de Transparencia (PNT): https://www.plataformadetransparencia.org.mx/web/guest/inicio, en Calle Lago Tequesquitengo #2600, colonia Lagos del Country, C.P. 45177 en Zapopan, Jalisco.

Cualquier cambio al presente aviso de privacidad se hará del conocimiento de los titulares de la información confidencial, a través de la página de internet de este sujeto obligado, la cual:https://transparencia.info.jalisco.gob.mx/sites/default/files/AVISO%20DE%20PRIVACIDAD%20COESIDA.pdf

El aviso de privacidad de la Coordinación Administrativa puede ser consultado en la siguiente liga:
https://transparencia.info.jalisco.gob.mx/sites/default/files/AVISO%20DE%20PRIVACIDAD%20FOCALIZADO%20COORDINACION%20DE%20ADMINISTRACION%20Y%20CONTABILIDAD.PDF#overlay-context=art%25C3%25ADculo-8-fracci%25C3%25B3n-

15 de diciembre del 2019

AVISO DE PRIVACIDAD FOCALIZADO
COORDINACIÓN DE ADMINISTRACIÓN Y CONTABILIDAD

El Consejo Estatal para la Prevención del Sida, con domicilio en Lago Tequesquitengo # 2600, Col Lagos del Country, C.P. 45177, Zapopan, Jalisco es la responsable del uso y protección de sus datos personales, y al respecto le informa lo siguiente:

Los datos personales se refieren a la información concerniente a una persona física identificada o identificable, y por datos personales sensibles, aquellos que afecten a la esfera más íntima de su titular o cuya utilización indebida puedan dar origen a discriminación o conlleve un riesgo grave para éste.

La protección de sus datos personales se realiza de conformidad a lo establecido en el artículo 6, Apartado A, fracción IV de la Constitución Política de los Estados Unidos Mexicanos, en los artículos 4 y 9 fracciones II, V y VI de la Constitución Política del Estado de Jalisco, en el artículo 30 fracción II y articulo 37 de la Ley General de Transparencia y Acceso a la Información Pública, artículo8 fracción V inciso ñ) e inciso p), articulo 34, articulo 35 de la Ley de Transparencia y Acceso a la Información Publica del Estado de Jalisco y sus Municipios, articulo 3.1 fracciones III y XXXII, articulo 10, articulo 19.2, articulo 24, articulo 87.1, fracciones I y X, articulo 90 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios, así como los artículos de la Ley de Compras Gubernamentales Enajenaciones y Contratación de Servicios del Estado de Jalisco y sus Municipios.

El tratamiento de sus datos personales se realiza de conformidad a lo establecido en las atribuciones de la Coordinación de Administración y Contabilidad dentro del Reglamento Interno de este Consejo en los artículos 48, 49, 50 y 51.

Los datos personales sensibles, se refieren a aquellos que requieren de especial protección como son: datos relacionados a la salud, ideológicos, de origen étnico o conlleve un riesgo grave para éste; Los datos personales se refieren a la información concerniente a una persona física identificada o identificable.

Los datos personales que serán sometidos a tratamiento son:

Datos Sensibles	**Datos Personales**
Huella digital Tipo de sangre Preferencia sexual Certificado médico	Nombre Fotografía Edad Fecha de Nacimiento Nacionalidad Estado Civil Domicilio Teléfono Sexo Grado máximo de estudios Correo electrónico Firma Peso Talla Datos académicos Datos Laborales Clave de Elector Imagen Corporal Registro Federal de Contribuyentes (RFC) Clave Única de Registro de Población (CURP) Numero de Seguridad Social (IMSS, ISSSTE) Carta de Policía Carta de No Sanción Administrativa Referencias (nombre, firma, teléfono)

Es importante apuntar que sus datos personales se consideran información confidencial, con excepción de su nombre, las relativas a la función que desempeña o la erogación de recursos públicos, y cualquier otra información que permita transparentar las acciones y garantizar el derecho a la información pública o que obre en fuentes de acceso público, en virtud de que constituye información susceptible de ser publicada y difundida.

Del mismo modo, usted podrá autorizar en cualquier momento la publicidad y difusión de los datos personales que se consideran confidenciales, incluyendo los sensibles, lo que deberá constar de manera escrita, expresa e inequívoca.

Los datos personales que usted proporcione al Consejo Estatal para la Prevención del Sida en Jalisco, serán única y exclusivamente utilizados para llevar a cabo los objetivos y atribuciones de esta dependencia y los utilizaremos para las siguientes finalidades:

Generar el expediente del personal, para el cumplimiento de las disposiciones administrativas como controles de acceso, contraseñas y medidas de seguridad, identificación y autentificación como servidor público, difusión de información pública de oficio, generar comprobantes de pago, cumplimiento de disposiciones fiscales y enteros de impuestos retenidos, remisión de constancias laborales, administrativas y de identificación; relativas al empleo, cargo o comisión, tales como el cumplimiento de los requisitos legales para la contratación y el pago de sueldos, salarios y prestaciones, historia laboral de los servidores públicos, cumplimiento de requisitos fiscales, administrativos y presupuestarios, altas, bajas y enteros en materias de seguridad social, aportaciones al Instituto de Pensiones del Estado, de identificación y localización del servidor público para fines laborales, administrativos y jurídicos, entradas y salidas del personal.

Se contemplan medidas especiales de protección en lo relativo al estado de salud y eventuales incapacidades, derivadas de riesgos de trabajo o enfermedades no profesionales.

Los datos personales recabados serán protegidos, incorporados y tratados en las bases de datos físicas y electrónicas de la Coordinación Administrativa del COESIDA.

Los datos personales que usted proporcione a la Coordinación Administrativa, serán única y exclusivamente utilizados para llevar a cabo los objetivos, finalidades y atribuciones de COESIDA y los utilizaremos para las siguientes finalidades:

- Llevar un registro público del padrón de proveedores de la Coordinación Administrativa, de conformidad con los artículos artículo 7° fracción I y artículo 8 numeral 1 fracción III de la Ley de Compras Gubernamentales Enajenaciones y Contratación de Servicios del Estado de Jalisco.

- Publicar la información concerniente a los concursos por invitación y licitaciones públicas en materia de adquisiciones, obra pública, proyectos de inversión y prestación de servicios, de conformidad con las obligaciones de Ley con respecto a la información fundamental obligatoria para todos los sujetos obligados, de conformidad con el artículo 8° fracción V incisos ñ) y p) de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios.

Este aviso de privacidad podrá sufrir modificaciones, los mismos que podrán ser consultados en la siguiente liga:

https://transparencia.info.jalisco.gob.mx/sites/default/files/AVISO%20DE%20PRIVACIDAD%20FOCALIZADO%20COORDINACION%20DE%20ADM!NISTRACION%20Y%20CONTABILIDAD.PDF#overlay-context=art%25C3%25ADculo-8-fracci%25C3%25B3n-

15 de diciembre del 2020

COESIDA
Consejo Estatal para
la Prevención del SIDA

Jalisco

SISTEMA DE CÁMARAS DE VIDEO VIGILANCIA

Usted está siendo video grabado con fines de seguridad por las cámaras del sistema de video vigilancia del Consejo Estatal para la Prevención del Sida (COESIDA), con domicilio en Lago Tequesquitengo # 2600, Col Lagos del Country, C.P. 45177, Zapopan, Jalisco; las imágenes y sonidos captados por las cámaras de video vigilancia serán utilizados con fines de control de acceso y salida de toda persona que ingrese al inmueble, incluidos personal de seguridad, limpieza, servidores públicos, prestadores de servicio social y visitantes.

Para mayor información sobre el uso de sus datos personales puede consultar nuestro aviso de privacidad integral en la siguiente liga:
https://transparencia.info.jalisco.gob.mx/sites/default/files/AVISO%20DE%20PRIVACIDAD%20COESIDA.pdf

COESIDA
Consejo Estatal para
la Prevención del SIDA

DOCUMENTO DE SEGURIDAD DEL CONSEJO ESTATAL PARA LA PREVENCIÓN DEL SIDA EN JALISCO

ÍNDICE

Los procedimientos de respaldo y recuperación de datos personales;

El plan de contingencia;

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

El plan de trabajo;

Los mecanismos de monitoreo y revisión de las medidas de seguridad, y

El programa general de capacitación

INTRODUCCIÓN

El Consejo Estatal para la Prevención del Síndrome de Inmunodeficiencia Adquirida (COESIDA), tiene el compromiso con los ciudadanos que sus datos personales serán tratados de una manera segura y eficaz, esto mediante un conjunto de procesos y sistemas diseñados para el fin de proteger los mismos. De esta manera se busca establecer, implementar, operar, monitorear y mejorar los procesos relativos a la adecuada protección, para así asegurar que no existe vulneración alguna a la confidencialidad, integridad y disponibilidad de la información. El Presente Documento de Seguridad, se realiza conforme lo prevé la Ley de Protección de Datos Personales en Posesión de Sujeto Obligados del Estado de Jalisco y sus Municipios, con el fin de asegurar la integridad, confidencialidad y disponibilidad de la información personal que éstos contienen.

El presente documento brinda al CONSEJO ESTATAL PARA LA PREVENCIÓN DEL SÍNDROME DE INMUNODEFICIENCIA ADQUIRIDA homogeneidad en la organización, procesos y sistemas, en el que el Comité de Transparencia, conjuntamente con el área de Informática y los responsables de los sistemas de datos personales, definen las medidas de seguridad administrativa, física y tecnológicas implementadas para la protección de los sistemas de datos personales custodiados.

Así mismo, este documento tiene como finalidad controlar internamente el proceso de sistemas de datos personales que posee el CONSEJO ESTATAL PARA LA PREVENCIÓN DEL SÍNDROME DE INMUNODEFICIENCIA ADQUIRIDA, el tipo de datos personales que contiene cada uno, los responsables, encargados, usuarios de cada sistema y las medidas de seguridad concretas implementadas.

GLOSARIO

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 éste. De manera enunciativa más 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.

Base 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.

Consentimiento: 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.

Documento de Seguridad: Instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee.

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

Evaluación de Impacto en la Protección de Datos Personales: Documento mediante el cual se valoran y determinan los impactos reales respecto de determinado tratamiento de datos personales, a efecto de identificar, prevenir y mitigar posibles riesgos que puedan comprometer el cumplimiento de los principios, deberes, derechos y demás obligaciones previstas en esta Ley y demás disposiciones aplicables.

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

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

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

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.

Responsable: Los sujetos obligados señalados en el artículo 1, párrafo 5, de la presente Ley que determinarán los fines, medios y alcance y demás cuestiones relacionadas con un tratamiento de datos personales.

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.

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.

Tratamiento: De manera enunciativa más 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

Catálogo de Sistemas de Tratamiento de Datos Personales.

SECRETARIO TÉCNICO

Sistema de Tratamiento de Control de Ingreso	
Administrador	Amelia Pérez Ramos
Cargo:	Apoyo Administrativo en Salud A7
Área	Secretario Técnico
Funciones y obligaciones ***Artículo 28 Capítulo V del Reglamento Interno***	**I.** Recibir, controlar y almacenar la correspondencia interna. **II.** Articular y almacenar el archivo. **III.** Atender llamadas telefónicas, así como apoyar con la recepción y remisión de información electrónica vía correo electrónico a otras áreas del Gobierno del Estado de Jalisco. **IV.** Recibir y clasificar, el archivo de trámite del área, para su debido registro y control. **V.** Atender las necesidades de recepción del personal adscrito. **VI.** Realizar el envío de la correspondencia. **VII.** Elaborar memorándum y oficios que se requieran en el área. **VIII.** Asistir a la coordinación de la reunión de vocalía **IX.** Las demás encomendadas por su superior jerárquico, así como las derivadas de la normatividad aplicable en la materia.
Personal autorizado para tratamiento	

Luis Alberto Ruiz Mora	Secretario Técnico
Tipos de datos personales pertenecientes al Sistema de Tratamiento de Control de Ingreso.	
Inventario	Nombre/Firma
Bases de datos	Electrónica y física
Controles de seguridad para las bases de datos	La información se reguarda en CPU con clave, así como archivero con llave, a los cuales únicamente tienen acceso las personas previamente autorizadas.
Estructura y descripción del Sistema de Tratamiento de Control de Ingreso.	
Tipo de soporte	Físico y Electrónico
Características del lugar del resguardo	Un archivero con cajoneras de, el cual tiene chapa, mismo que se encuentra en la oficina de la asistente del Secretario Técnico.
Programas en que se utilizan los Datos Personales.	No aplica
Las bitácoras de acceso y operación cotidiana	
Bitácoras Físicas e Identificación y/o lugar de almacenamiento.	Registros
Bitácoras electrónicas e Identificación y/o lugar de almacenamiento.	Las bitácoras electrónicas de acceso a los datos personales se encuentran en posesión y resguardo de la asistente del Secretario Técnico, la cual tiene la obligación de documentar los accesos que se den a la información.
Las bitácoras de vulneraciones de seguridad	
Cuando exista un intento o bien una vulneración de los datos personales está deberá quedar documentada en la bitácora de vulneraciones de seguridad.	
Medidas de seguridad físicas aplicadas a las instalaciones	

Acceso al espacio de trabajo, así también como al equipo de cómputo solo por el personal autorizado.

Sistema de Tratamiento de Expedientes de Solicitudes de Acceso a la Información Pública y Protección de Datos Personales y Recursos Correspondientes	
Administrador	Sorhaya Carolina Salazar Arroyo
Cargo:	Titular de la Unidad de Transparencia
Área	Secretario Técnico
Funciones y obligaciones ***Artículo 28 Capítulo V del Reglamento Interno***	I. Administrar el sistema del sujeto obligado que opere la información fundamental; II. Actualizar mensualmente la información fundamental del sujeto obligado; III. Recibir y dar respuesta a las solicitudes de información pública, para lo cual debe integrar el expediente, realizar los trámites internos y desahogar el procedimiento respectivo; IV. Tener a disposición del público formatos para presentar solicitudes de información pública: a) Por escrito; b) Para imprimir y presentar en la Unidad, y c) Vía internet; V. Llevar el registro y estadística de las solicitudes de información pública VI. Requerir y recabar de las oficinas correspondientes o, en su caso, de las personas físicas que hubieren recibido recursos públicos o realizado actos de autoridad, la información pública de las solicitudes procedentes; VII. Solicitar al Comité de Transparencia interpretación o modificación de la clasificación de información pública solicitada; VIII. Capacitar al personal de las oficinas del sujeto obligado.

	XI. Informar al titular del sujeto obligado y al Instituto sobre la negativa de los encargados de las oficinas del sujeto obligado para entregar información pública de libre acceso; X. Proponer al Comité de Transparencia procedimientos internos que aseguren la mayor eficiencia en la gestión de las solicitudes de acceso a la información; XI. Coadyuvar con el sujeto obligado en la promoción de la cultura de la transparencia y el acceso a la información pública; XII. Las demás encomendadas por su superior jerárquico, así como las derivadas de la normatividad aplicable en la materia.
Personal autorizado para tratamiento	
Luis Alberto Ruiz Mora	Secretario Técnico
Tipo de datos personales pertenecientes al Sistema de tratamiento de expedientes de solicitudes de acceso a la información pública y protección de datos personales y recursos correspondientes.	
Inventario	Nombre, domicilio, firma, correo electrónico, teléfono
Bases de datos	N/A
Controles de seguridad para las bases de datos	La información se reguarda en archiveros con llave, a los cuales únicamente tienen acceso las personas previamente autorizadas.
Estructura y descripción del Sistema de Tratamiento de asesoría jurídica y capacitación a los sujetos obligados.	
Tipo de soporte	Físico y Electrónico.
Características del lugar del resguardo	Escritorio con cajones los cuales cuentan con chapa, mismo que se encuentra en el área de trabajo de la Titular de la Unidad, USB.
Programas en que se utilizan los Datos Personales.	N/A
Las bitácoras de acceso y operación cotidiana	
Bitácoras Físicas e Identificación y/o lugar de almacenamiento.	No aplica

Bitácoras electrónicas de Identificación y/o lugar de almacenamiento.	Existe una base de datos en formato Excel, el cual es resguardado en la computadora del Titular de la Unidad, en la cual se hace constar el nombre de los solicitantes y recurrentes
Las bitácoras de vulneraciones de seguridad	
Cuando exista un intento o bien una vulneración a los datos personales esta deberá quedar documentada en la bitácora de vulneraciones de seguridad.	
Medidas de seguridad físicas aplicadas a las instalaciones	
Acceso al espacio de trabajo, así también como al equipo de cómputo solo por el personal autorizado.	

COORDINADOR DE SUBCONSEJOS

Sistema de Tratamiento de Subconsejos	
Administrador	Dr. Jorge Raúl Sánchez Biorato
Cargo:	Coordinador de Subconsejos
Área	Atención Integral/ Área de Manejo y Distribución e Inventario de Medicamentos Antirretrovirales/Evaluación y Seguimiento/Derechos Humanos/Prevención/
Funciones y obligaciones ***Artículo 33, 34 y 35 Capítulo VI del Reglamento Interno***	I. Aplicación de pruebas de VIH/Sífilis II. Valoración médica, psicológica, laboratorial y ministración de medicamentos. II. Incorporación al programa de la Secretaria de Salud a los pacientes con Seguro Popular para el otorgamiento de consulta médica y tratamiento de antirretrovirales. V. Registro en el Sistema de Administración y Logística de Antirretrovirales (SALVAR) para el seguimiento laboratorial (Carga Viral y CD4). V. Comunicación e información sobre adherencia al tratamiento. VI. Abasto y Distribución de Medicamentos Antirretrovirales en los Servicios de Atención Integral (SAI´s). VII. Actualizaciones el Sistema de Administración, Logística de Antirretrovirales (SALVAR)

	VIII. Derivación de pacientes con Seguridad Social para la pronta atención medica de los pacientes de nuevo diagnóstico y reincorporación. IX. Aplicación de muestras para conteo de Linfocitos T CD4+, Carga Viral y Genotipo de VIH para pacientes de nuevo diagnóstico para el protocolo E02-17 (INER). X. Atención a usuarios para la atención al protocolo ImPrEP. XI. Seguimiento a mujeres embarazadas de nuevo diagnóstico para el acompañamiento de su atención medica hasta su alumbramiento. XII. Cursos de capacitación de prevención de VIH, sida, ITS; estigma y discriminación. promoción de estrategias de prevención. XIII. Distribución de folletería, promocionales y preservativos. XIV. Integración de mesas de trabajo XV. Calendarización de órdenes de requisición para promocionales y folletería. XVI. Coordinación con las Instituciones y población en general para impartir platicas de información sobre VIH/sida e ITS. XVII. Planeación y Captura en la plataforma para la requisición del presupuesto. XVIII. Validación de indicadores. XIX. Captura, seguimiento y monitoreo de información

Personal autorizado para tratamiento	
Dr. Jorge Raúl Sánchez Biorato	Coordinador
Dr. Juan Rivera Romero	Área de Manejo y Distribución e Inventario de Medicamentos Antirretrovirales.
Sergio Eduardo Hernández Guerrero	Entrega de Medicamentos Antirretrovirales en los Servicios de Atención Integral (SAI´s)
Lic. Adriana Núñez	Seguimiento a mujeres embarazadas de nuevo diagnóstico.

Lic. Martha Villalobos De la Mora	Cursos de capacitación
Lic. Marisela Sánchez	Mesas de trabajo con las Instituciones y ONG´s
Lic. Josefina del Sagrario López Navarro	Platicas de información
Lic. Teresa Leal	Investigación, Evaluación y Seguimiento.

Funciones:

- Promover, participar y difundir las investigaciones sobre VIH/sida en el Estado.
- Originar mejorías en atención médica de las personas que viven con VIH/sida, a través de la implementación y fortalecimiento del modelo de atención integral, en coordinación con las diferentes instituciones involucradas en el manejo de los pacientes.
- Administrar los recursos humanos, materiales y de equipo asignados para la ejecución del programa a cargo del COESIDA.
- Impulsar acuerdos de colaboración entre instituciones, organismos de la sociedad civil y privados, que fortalezcan las estrategias de prevención del VIH, derechos humanos y atención integral de las personas que viven con VIH o SIDA en el Estado.

Tipo de datos personales pertenecientes al Subconsejo de Atención Integral a los sujetos obligados.	
Inventario	Nombre, domicilio, CURP, teléfono, estado de salud. Nacionalidad, lugar y fecha de nacimiento.
Bases de datos	Excel
Controles de seguridad para las bases de datos	ELIMINADO: un renglones, Información Reservada Artículo 17.1 fracción I inciso a) LTAIPEJM Controles de seguridad

Estructura y descripción del Sistema de Tratamiento del Subconsejo de Atención Integral a los sujetos obligados.	
Tipo de soporte	Físico y Electrónico.
Características del lugar del resguardo	Archiveros con cajoneras, escritorio con cajón, los cuales cuentan con chapa, mismos que se encuentran en cada lugar de trabajo de los sujetos obligados, así también como USB.

Programas en que se utilizan los Datos Personales.	Sistema de Administración, Logística y Vigilancia de ARV (SALVAR) Excel Formato de Consentimiento de búsqueda Formato de expediente para pacientes con IMSS Formato de expediente para pacientes Migrantes
Las bitácoras de acceso y operación cotidiana	
Bitácoras Físicas e Identificación y/o lugar de almacenamiento.	Están bajo resguardo de cada sujeto obligado.
Bitácoras electrónicas de Identificación y/o lugar de almacenamiento.	Las bitácoras electrónicas de acceso a los datos personales se encuentran en posesión y resguardo de cada sujeto obligado, el cual tiene la obligación de documentar los accesos que se den a la información.
Las bitácoras de vulneraciones de seguridad	
Cuando exista un intento o bien una vulneración a los datos personales esta deberá quedar documentada en la bitácora de vulneraciones de seguridad.	

Sistema de Tratamiento de Subconsejos	
Administrador	Dra. Claudia Canobbio
Cargo:	Médico General
Área	Programa de Detección Integral e Incorporación a Usuarios a los Servicios de Salud
Funciones y obligaciones ***Artículo 33, 34 y 35 Capítulo VI del Reglamento Interno***	I. Orientación y acompañamiento de pacientes a los Servicios de Atención Integra (SAI´s) con Seguro Popular para su atención médica. II. Llenado de formatos para el conteo de Linfocitos T CD4+ Carga Viral, Hepatitis, VDR para confirmación de resultados. III. Aplicación de muestras para conteo de Linfocitos T CD4+, Carga Viral y Genotipo de VIH para pacientes de nuevo diagnóstico para el protocolo E02-17 (INER).

Personal autorizado para tratamiento	
Dr. Jorge Raúl Sánchez Biorato	Programa de Detección Integral e Incorporación a Usuarios a los Servicios de Salud
Tipo de datos personales pertenecientes al Subconsejo de Atención Integral a los sujetos obligados.	
Inventario	Nombre, Identificación oficial, correo electrónico, teléfono, datos de salud, Numero de póliza de Seguro Popular, referencia familiar (nombre y teléfono)
Bases de datos	Excel
Controles de seguridad para las bases de datos	ELIMINADO un renglones, Información Reservada Artículo 17.1 fracción I inciso a) LTAIPEJM Controles de seguridad
Estructura y descripción del Sistema de Tratamiento del Subconsejo de Atención Integral a los sujetos obligados.	
Tipo de soporte	Físico y Electrónico.
Características del lugar del resguardo	Archiveros con cajoneras, escritorio con cajón, los cuales cuentan con chapa, mismos que se encuentran en cada lugar de trabajo de los sujetos obligados, así también como USB.
Programas en que se utilizan los Datos Personales.	Excel Formato de Consentimiento de búsqueda
Las bitácoras de acceso y operación cotidiana	
Bitácoras Físicas e Identificación y/o lugar de almacenamiento.	Están bajo resguardo de cada sujeto obligado.
Bitácoras electrónicas de Identificación y/o lugar de almacenamiento.	Las bitácoras electrónicas de acceso a los datos personales se encuentran en posesión y resguardo de cada sujeto obligado, el cual tiene la obligación de documentar los accesos que se den a la información.
Las bitácoras de vulneraciones de seguridad	

Cuando exista un intento o bien una vulneración a los datos personales esta deberá quedar documentada en la bitácora de vulneraciones de seguridad.

Técnicas de supresión y borrado seguro de datos personales	
Métodos físicos	**Trituración mediante corte horizontal:** Cortar el documento de forma horizontal generando fragmentos diminutos, lo cual hace prácticamente imposible que se puedan unir. **Destrucción de los medios de almacenamiento electrónicos:** Mediante desintegración, consistente en separación completa o pérdida de la unión de los elementos que conforman algo.
Métodos Lógicos	**Sobre-escritura:** Consiste en sobrescribir todas las ubicaciones de almacenamiento utilizables en un medio de almacenamiento, es decir, se trata de escribir información nueva en la superficie de almacenamiento, en el mismo lugar que los datos existentes, utilizando herramientas de software.

Análisis de riesgo

La Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios distingue en su artículo 38 las siguientes vulneraciones de seguridad de la información confidencial:

- La pérdida o destrucción no autorizada;
- El robo, extravío o copia no autorizada;
- El uso, acceso o tratamiento no autorizado; o
- El daño, la alteración o modificación no autorizada.

Tomando en cuenta las circunstancias generales y actuales, tanto físicas como humanas, de este sujeto obligado donde se tratan los datos personales recabados de las funciones de la administración pública, hemos logrado identificar los siguientes riesgos posibles ante los que se pudiera enfrentar este Sujeto Obligado:

ELIMINADO: párrafo, Información Reservada Artículo 17.1 fracción I inciso a) LTAIPEJM. Medidas de seguridad faltantes. Su publicación pondría en riesgo al organismo pues reflejaría las posibles vulnerabilidades.

[redacted]

ELIMINADO: párrafo, Información Reservada Artículo 17.1 fracción I inciso a) LTAIPEJM. Medidas de seguridad faltantes. Su publicación pondría en riesgo al organismo pues reflejaría las posibles vulnerabilidades

[redacted]

[redacted]

[redacted]

ELIMINADO: párrafo, Información Reservada Artículo 17.1 fracción I inciso a) LTAIPEJM. Medidas de seguridad faltantes. Su publicación pondría en riesgo al organismo pues reflejaría las posibles vulnerabilidades

ELIMINADO: párrafo, Información Reservada Artículo 17.1 fracción I inciso a) LTAIPEJM. Medidas de seguridad faltantes. Su publicación pondría en riesgo al organismo pues reflejaría las posibles vulnerabilidades

Análisis de brecha

Una vez identificados los posibles riesgos a los que este Sujeto Obligado se encuentra susceptible de enfrentar, podemos realizar el análisis de brecha, utilizando como base los inventarios de datos personales que se hicieron con cada área.

Las diferentes direcciones reportaron las siguientes medidas de seguridad existentes:

ELIMINADO: párrafo, Información Reservada Artículo 17.1 fracción I inciso a) LTAIPEJM. Medidas de seguridad faltantes. Su publicación pondría en riesgo al organismo pues reflejaría las posibles vulnerabilidades

ELIMINADO: párrafo, Información Reservada Artículo 17.1 fracción I inciso a) LTAIPEJM. Medidas de seguridad faltantes. Su publicación pondría en riesgo al organismo pues reflejaría las posibles vulnerabilidades

Plan de Trabajo
La existencia del documento de seguridad, busca enmarcar los deberes, para la óptima protección de datos personales; en ese sentido, debido a la importancia en materia de datos personales, se debe mantener actualizado el plan de trabajo, el cual permita alcanzar los objetivos del sistema de seguridad. Con base en lo anterior, se ha planteado implementar la totalidad de las medidas de seguridad faltantes en un periodo de dieciocho meses a partir de la aprobación del presente documento de seguridad; con base en lo anterior, las medidas de seguridad físicas y técnicas que requieran la erogación de recursos, se realizarán conforme a los tiempos administrativos y el presupuesto lo permita. Para la ejecución del presente documento de seguridad, se dará prioridad a las siguientes actividades:

Ante la pérdida total o parcial de datos personales en posesión de este sujeto obligado, se debe contar con un plan de contingencia, que nos permita dar continuidad a la aplicación de este documento de seguridad, así como enfrentarnos a fallas y eventos inesperados que podrían derivar en la pérdida parcial o total de la información confidencial que posee este sujeto obligado.

Con la evaluación de riesgos y la elaboración de las medidas de seguridad aplicables para prevenir las posibles vulneraciones y daños a los que nos encontramos expuestos, nos encontramos con que el plan de contingencias de este sujeto obligado consiste en la aplicación de las medidas de seguridad tratadas en el apartado anterior, mismas que están sujetas a cambios por eventualidades no contempladas, por ello la importancia de señalar que el presente se trata de un plan de contingencia no limitativo.

Lo anterior toda vez que en la actualidad existen cambios y grandes avances que van modificando la organización de la información, y al igual existen riesgos inminentes que día a día evoluciona.

En caso de cualquier vulneración o daño a la seguridad de los datos personales, se deberá actuar con eficiencia, de forma rápida y oportuna, así como en todo momento procurar minimizar el daño, asegurando tener las menores pérdidas posibles y buscando la mayor recuperación de la información en el menor tiempo y costo posible para la dependencia.

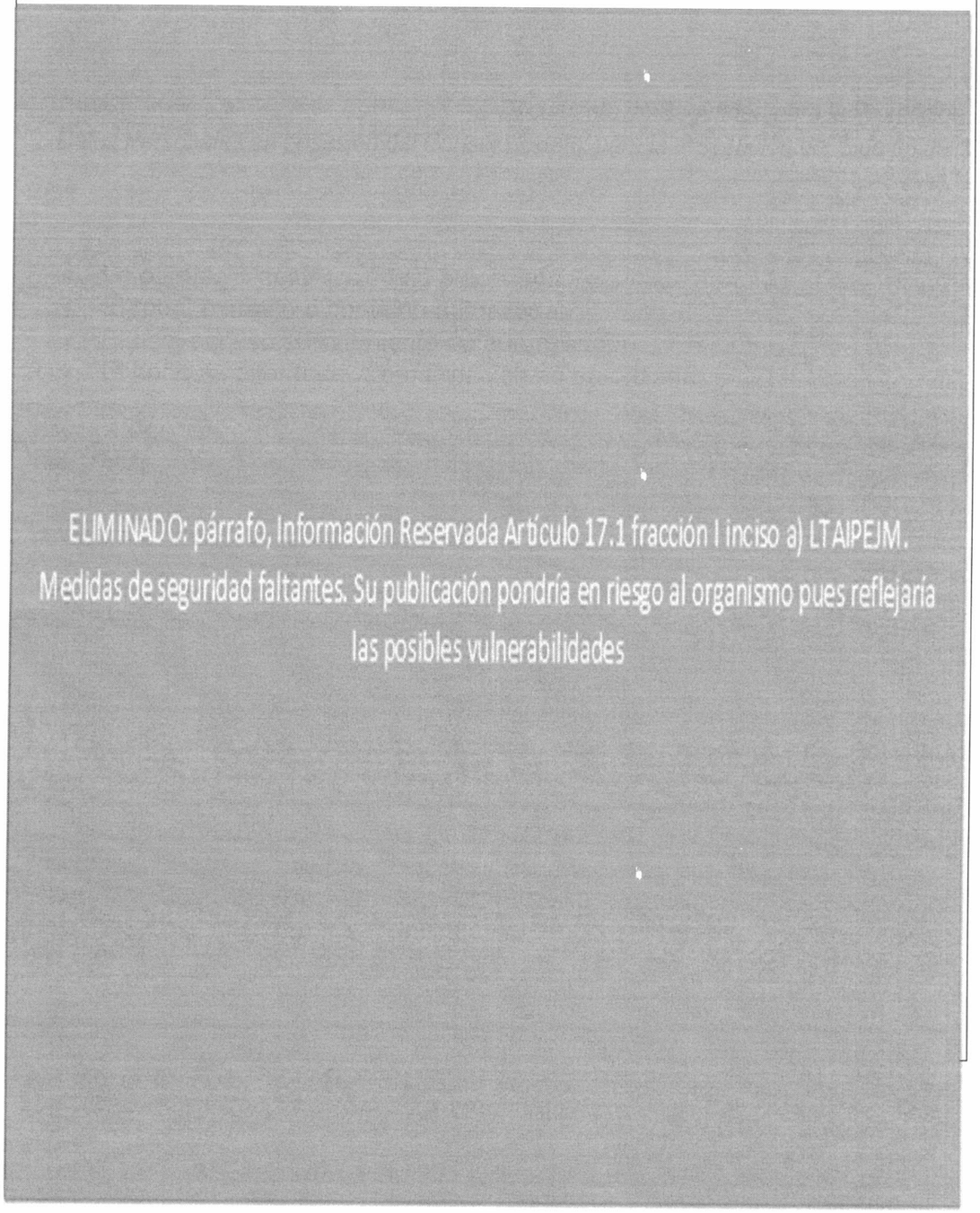
En caso de que los datos personales sufran algún tipo de daño o pérdida, se dispondrá de los respaldos electrónicos realizados por cada dirección en donde se contienen copias de documentos y/o archivos y/o bases de datos que contienen datos personales que permitirían restablecer los datos a la fecha del último respaldo.

Sistema de Tratamiento de Subconsejos	
Administrador	Ancira Donai Dueñas Martínez Erika Trinidad Canchola López
Cargo:	Apoyo Administrativo en Salud A9 Enfermera Especialista
Área	Derechos Humanos, Vinculación a pacientes con IMSS e ISSSTE e Inmigrantes

Funciones y obligaciones ***Artículo 33, 34 y 35 Capítulo VI del Reglamento Interno***	I. Derivación de pacientes con Seguridad Social (IMSS e ISSSTE) tanto de nuevo diagnostico como reincorporación para la pronta atención medica en las Instituciones de Salud. II. Orientación y acompañamiento a usuarios y/o pacientes que viven con situaciones de discriminación y violación a sus derechos humanos tanto por negación de la atención por instituciones y personal de salud, violación a la confidencialidad y maltrato. III. Aplicación de muestras para conteo de Linfocitos T CD4+, Carga Viral y Genotipo de VIH para pacientes de nuevo diagnóstico para el protocolo E02-17 (INER).
Personal autorizado para tratamiento	
Dr. Jorge Raúl Sánchez Biorato	Derechos Humanos, Vinculación a pacientes con IMSS e ISSSTE e Inmigrantes
Tipo de datos personales pertenecientes al Subconsejo de Atención Integral a los sujetos obligados.	
Inventario	Nombre, CURP, correo electrónico, teléfono, datos de salud, numero de seguridad social, estatus de migración
Bases de datos	Excel
Controles de seguridad para las bases de datos	ELIMINADO: un renglones, Información Reservada Artículo 17.1 fracción I inciso a) LTAIPEJM. Controles de seguridad
Estructura y descripción del Sistema de Tratamiento del Subconsejo de Atención Integral a los sujetos obligados.	
Tipo de soporte	Físico y Electrónico.
Características del lugar del resguardo	Archiveros con cajoneras, escritorio con cajón, los cuales cuentan con chapa, mismos que se encuentran en cada lugar de trabajo de los sujetos obligados, así también como USB.

Programas en que se utilizan los Datos Personales.	Excel Formato de expediente para pacientes con IMSS Formato de expediente para pacientes Migrantes
Las bitácoras de acceso y operación cotidiana	
Bitácoras Físicas e Identificación y/o lugar de almacenamiento.	Están bajo resguardo de cada sujeto obligado.
Bitácoras electrónicas de Identificación y/o lugar de almacenamiento.	Las bitácoras electrónicas de acceso a los datos personales se encuentran en posesión y resguardo de cada sujeto obligado, el cual tiene la obligación de documentar los accesos que se den a la información.
Las bitácoras de vulneraciones de seguridad	
Cuando exista un intento o bien una vulneración a los datos personales esta deberá quedar documentada en la bitácora de vulneraciones de seguridad.	
Técnicas de supresión y borrado seguro de datos personales	
Métodos físicos	**Trituración mediante corte horizontal:** Cortar el documento de forma horizontal generando fragmentos diminutos, lo cual hace prácticamente imposible que se puedan unir.
Métodos Lógicos	**Destrucción de los medios de almacenamiento electrónicos:** Mediante desintegración, consistente en separación completa o pérdida de la unión de los elementos que conforman algo. **Sobre-escritura:** Consiste en sobrescribir todas las ubicaciones de almacenamiento utilizables en un medio de almacenamiento, es decir, se trata de escribir información nueva en la superficie de almacenamiento, en el mismo lugar que los datos existentes, utilizando herramientas de software.
Análisis de riesgo	
La Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios distingue en su artículo 38 las siguientes vulneraciones de seguridad de la información confidencial:	

- La pérdida o destrucción no autorizada;
- El robo, extravío o copia no autorizada;
- El uso, acceso o tratamiento no autorizado; o
- El daño, la alteración o modificación no autorizada.



electrónicos que contengan datos	Acceder a información o datos personales, mediante el acceso no autorizado.

ELIMINADO: párrafo, Información Reservada Artículo 17.1 fracción I inciso a) LTAIPEJM. Medidas de seguridad faltantes. Su publicación pondría en riesgo al organismo pues reflejaría las posibles vulnerabilidades

	Falla en equipos.

ELIMINADO. Información Reservada Artículo 17.1 fracción I inciso a) LTAIPEJM. Análisis de riesgo de los datos en posesión del organismo, puede poner en riesgo a los datos personales por la divulgación del mismo.

Análisis de brecha
Una vez identificados los posibles riesgos a los que este Sujeto Obligado se encuentra susceptible de enfrentar, podemos realizar el análisis de brecha, utilizando como base los inventarios de datos personales que se hicieron con cada área.

ELIMINADO: párrafo, Información Reservada Artículo 17.1 fracción I inciso a) LTAIPEJM. Medidas de seguridad faltantes. Su publicación pondría en riesgo al organismo pues reflejaría las posibles vulnerabilidades

ELIMINADO: párrafo, Información Reservada Artículo 17.1 fracción I inciso a) LTAIPEJM. Medidas de seguridad faltantes. Su publicación pondría en riesgo al organismo pues reflejaría las posibles vulnerabilidades

ciudadanos, es decir en el espacio físico donde se recaban los datos personales.

Sistema de Tratamiento de Subconsejos	
Administrador	Dr. Ricardo Ramírez Mora
Cargo:	Médico General
Área	Genotipo de VIH para pacientes de nuevo diagnóstico para el protocolo E02-17 (INER).
Funciones y obligaciones ***Artículo 33, 34 y 35 Capítulo VI del Reglamento Interno***	I. Llenado de formatos para la aplicación de muestras para conteo de Linfocitos T CD4+, Carga Viral y Genotipo de VIH para pacientes de nuevo diagnóstico para el protocolo E02-17 (INER). II. Llenado de estudio epidemiológico que en envía a la Secretaria de Salud
Personal autorizado para tratamiento	
Dr. Jorge Raúl Sánchez Biorato	Coordinador de Subconsejos

Tipo de datos personales pertenecientes al Subconsejo de Atención Integral a los sujetos obligados.	
Inventario	Nombre, correo electrónico, teléfono, datos de salud
Bases de datos	Excel
Controles de seguridad para las bases de datos	ELIMINADO: un renglones, Información Reservada Artículo 17.1 fracción I inciso a) LTAIPEJM. Controles de seguridad.
Estructura y descripción del Sistema de Tratamiento del Subconsejo de Atención Integral a los sujetos obligados.	
Tipo de soporte	Físico y Electrónico.
Características del lugar del resguardo	Escritorio con cajón, los cuales cuentan con chapa, mismos que se encuentran en cada lugar de trabajo de los sujetos obligados, así también como USB.
Programas en que se utilizan los Datos Personales.	Excel Formato de Consentimiento de búsqueda
Las bitácoras de acceso y operación cotidiana	
Bitácoras Físicas e Identificación y/o lugar de almacenamiento.	Están bajo resguardo de cada sujeto obligado.
Bitácoras electrónicas de Identificación y/o lugar de almacenamiento.	Las bitácoras electrónicas de acceso a los datos personales se encuentran en posesión y resguardo de cada sujeto obligado, el cual tiene la obligación de documentar los accesos que se den a la información.
Las bitácoras de vulneraciones de seguridad	
Cuando exista un intento o bien una vulneración a los datos personales esta deberá quedar documentada en la bitácora de vulneraciones de seguridad.	
Técnicas de supresión y borrado seguro de datos personales	
Métodos físicos	**Trituración mediante corte horizontal:** Cortar el documento de forma horizontal generando fragmentos diminutos, lo cual hace prácticamente imposible que se puedan unir.

Métodos Lógicos	**Destrucción de los medios de almacenamiento electrónicos:** Mediante desintegración, consistente en separación completa o pérdida de la unión de los elementos que conforman algo. **Sobre-escritura:** Consiste en sobrescribir todas las ubicaciones de almacenamiento utilizables en un medio de almacenamiento, es decir, se trata de escribir información nueva en la superficie de almacenamiento, en el mismo lugar que los datos existentes, utilizando herramientas de software.

Análisis de riesgo

La Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios distingue en su artículo 38 las siguientes vulneraciones de seguridad de la información confidencial:

- La pérdida o destrucción no autorizada;
- El robo, extravío o copia no autorizada;
- El uso, acceso o tratamiento no autorizado; o
- El daño, la alteración o modificación no autorizada.

ELIMINADO: párrafo, Información Reservada Artículo 17.1 fracción I inciso a) LTAIPEJM. Medidas de seguridad faltantes. Su publicación pondría en riesgo al organismo pues reflejaría las posibles vulnerabilidades

- Diligencias inadecuadas, malas prácticas de los servidores públicos en relación a la confidencialidad que deben guardar sobre los datos personales que conozcan y traten debido al desempeño de sus funciones.
- Pérdida, robo o extravío de expedientes integrados con datos personales.
- Alteración de la información respecto a los datos personales.

ELIMINADO: párrafo, Información Reservada Artículo 17.1 fracción I inciso a) LTAIPEJM. Medidas de seguridad faltantes. Su publicación pondría en riesgo al organismo pues reflejaría las posibles vulnerabilidades

	• Fuego. • Accidentes. • Corrosión.
Eventos naturales.	Desastres climatológicos. Fenómenos meteorológicos.

ELIMINADO: párrafo, Información Reservada Artículo 17.1 fracción I inciso a) LTAIPEJM. Medidas de seguridad faltantes. Su publicación pondría en riesgo al organismo pues reflejaría las posibles vulnerabilidades

Una vez identificados los posibles riesgos a los que este Sujeto Obligado se encuentra susceptible de enfrentar, podemos realizar el análisis de brecha, utilizando como base los inventarios de datos personales que se hicieron con cada área.

Las diferentes direcciones reportaron las siguientes medidas de seguridad existentes:

ELIMINADO: párrafo, Información Reservada Artículo 17.1 fracción I inciso a) LTAIPEJM. Medidas de seguridad faltantes. Su publicación pondría en riesgo al organismo pues reflejaría las posibles vulnerabilidades

Sistema de Tratamiento de Subconsejos	
Administrador	Lic Luz María Dueñas Olvera Dr Alberto Plascencia
Cargo:	Psicóloga Clínica Médico General
Área	Profilaxis Post Exposición – PEP/No Ocupacional Profilaxis Post Exposición – PEP/Ocupacional

Funciones y obligaciones ***Artículo 33, 34 y 35*** ***Capítulo VI del Reglamento Interno***	I. Llenado de formato "Consentimiento para participar en el Programa de Medicamentos Antirretrovirales para Profilaxis Post-exposición no ocupacional al VIH del COESIDA. II. Llenado de Consentimiento Informado y De Búsqueda para Profilaxis Post Exposición – PEP/Ocupacional, anexando oficio de parte de infectologo informando sobre el accidente, así como el tratamiento que necesitará.
Personal autorizado para tratamiento	
Dr. Jorge Raúl Sánchez Biorato	Coordinador de Subconsejos
Tipo de datos personales pertenecientes al Subconsejo de Atención Integral a los sujetos obligados.	
Inventario	Nombre, correo electrónico, teléfono, datos de salud, código postal
Bases de datos	Excel
Controles de seguridad para las bases de datos	ELIMINADO: un renglones, Información Reservada Artículo 17.1 fracción I inciso a) LTAIPEJM. Controles de seguridad
Estructura y descripción del Sistema de Tratamiento del Subconsejo de Atención Integral a los sujetos obligados.	
Tipo de soporte	Físico y Electrónico.
Características del lugar del resguardo	Escritorio con cajón, los cuales cuentan con chapa, mismos que se encuentran en cada lugar de trabajo de los sujetos obligados, así también como USB.
Programas en que se utilizan los Datos Personales.	Excel Formato de Consentimiento de búsqueda
Las bitácoras de acceso y operación cotidiana	

Bitácoras Físicas e Identificación y/o lugar de almacenamiento.	Están bajo resguardo de cada sujeto obligado.
Bitácoras electrónicas de Identificación y/o lugar de almacenamiento.	Las bitácoras electrónicas de acceso a los datos personales se encuentran en posesión y resguardo de cada sujeto obligado, el cual tiene la obligación de documentar los accesos que se den a la información.
Las bitácoras de vulneraciones de seguridad	
Cuando exista un intento o bien una vulneración a los datos personales esta deberá quedar documentada en la bitácora de vulneraciones de seguridad.	

Sistema de Tratamiento de la Coordinación Administrativa	
Administrador	Lic. Aída María de Jesús Jiménez Jiménez
Cargo:	Coordinación Administrativa
Área	Coordinación Administrativa
Funciones y obligaciones ***Artículo 48,49,51 Sesión Cuarta del Reglamento Interno***	**I.** Presupuestos históricos ejercidos. **II.** Planificar un presupuesto para un lapso determinado de tiempo. **III.** Elaborar un anteproyecto de Presupuesto Anual y costea procesos operativos programados. **IV.** Elaborar un cronograma de compras en base a proyectos. **V.** Suministrar materiales e insumos al área operativa. **VI.** Promociona plazas vacantes a personal interno y/o promueve contratación de recurso humano. **VII.** Determinar los tipos de documentos que deben existir en la organización para garantizar que los procesos se lleven a cabo bajo condiciones controladas. **VIII.** Contratación, entrega de información y formatos administrativos para su manejo dentro de la Institución.

	IX. Establecer todos los elementos generales necesarios para la elaboración del Sistema Documental.
Personal autorizado para tratamiento	
Aida María de Jesús Jiménez Jiménez Carlos Felipe Rivera Fragoso	Coordinadora Administrativa Apoyo Administrativo en Salud A8
Tipo de datos personales pertenecientes al Sistema de Tratamiento de Recursos Humanos y Materiales.	
Inventario	Nombre, domicilio, correo electrónico, firma, teléfono (fijo y celular), fotografía, CURP, RFC, fecha de nacimiento, INE, datos de salud, nombres de familiares, datos académicos y datos laborales, huella digital, imagen corporal, Curriculum Vitae,
Base de datos	**I.** Nombre de empleado **II.** RFC **III.** CURP **IV.** Domicilio **V.** Teléfono **VI.** Huella Digital **VII.** Imagen Corporal
Número de Titulares	Aída María de Jesús Jiménez Jiménez Carlos Felipe Rivera Fragoso
Controles de seguridad para las bases de datos	ELIMINADO: un renglones, Información Reservada Artículo 17.1 fracción I inciso a) LTAIPEJM. Controles de seguridad
Estructura y descripción del Sistema de Tratamiento de Recursos Humanos y Materiales.	
Tipo de soporte	Físico y Electrónico.

Características del lugar del resguardo	Archivero con cajones de color blanco, el cual tiene chapa, mismo que se encuentra debajo del escritorio asignado a su cargo.
Programas en que se utilizan los Datos Personales.	Existe una base de datos en formato Excel, el cual es resguardado en la computadora del Coordinador Administrativo. Así mismo se cuenta con expediente físico de cada uno de los empleados, en resguardo de archivo con llave.
Las bitácoras de acceso y operación cotidiana	
Bitácoras Físicas e Identificación y/o lugar de almacenamiento.	Las bitácoras electrónicas de acceso a los datos personales se encuentran en posesión y resguardo del Coordinador Administrativo, la cual tiene la obligación de documentar los accesos que se den a la información.
Bitácoras electrónicas e Identificación y/o lugar de almacenamiento.	Las bitácoras electrónicas de acceso a los datos personales se encuentran en posesión y resguardo del Coordinador Administrativo, la cual tiene la obligación de documentar los accesos que se den a la información.
Las bitácoras de vulneraciones de seguridad	
Cuando exista un intento o bien una vulneración de las medidas de seguridad, este deberá quedar documentado en la bitácora de vulneraciones de seguridad.	

CONTROLES Y MECANISMOS DE SEGURIDAD PARA LAS TRANSFERENCIAS

Transmisiones de Datos Personales mediante Soportes Físico

1. El envío se realiza a través de personal de Recepción el cual deberá ser autorizado por su superior jerárquico mediante acuse sello y firma de recibido.
2. Cuando se transfiere información confidencial esta se realiza en sobres se utiliza la leyenda de clasificación señalada en los Lineamientos Generales para Clasificación y Desclasificación de la Información, así como para la Elaboración de las Versiones Públicas;
3. La información sólo es entregada a los titulares de la información o sus autorizados, previa acreditación con identificación oficial

4. Toda entrega de información requiere acuse de recibo, e identificación.

Transmisiones mediante el traslado físico de soportes electrónicos

1. Cuando se transfiere información confidencial esta se realiza en sobres sellados y se utiliza la leyenda de clasificación señalada en los Lineamientos Generales para Clasificación y Desclasificación de la Información, así como para la Elaboración de las Versiones Públicas;
2. La información sólo es entregada a los titulares de la información o sus autorizados, previa acreditación con identificación oficial
3. Toda entrega de información requiere acuse de recibo, y
4. Las transmisiones serán registradas en las bitácoras de transferencia de cada área.

Transferencias

☒Interinstitucionales
☐Internacionales
☐Con entes privados

Tipo de Traslado

☒De soportes físicos
☒Físico de soportes electrónicos
☐Sobre redes electrónicas

BITÁCORAS DE ACCESO, OPERACIÓN COTIDIANA Y VULNERACIONES A LA SEGURIDAD DE LOS DATOS PERSONALES

Bitácoras de Acceso

Las bitácoras de acceso a los datos personales se utilizan en los soportes Físicos, mismas que se encontraran a resguardo del encargado de cada área donde se traten datos personales, dichas bitácoras contienen la siguiente información:

Anexo, Bitácora de Acceso

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

Bitácoras de Vulneraciones a la Seguridad de los Datos Personales

Las bitácoras de vulneración de datos personales se utilizan en los soportes Físicos, mismas que se encontraran a resguardo del encargado de cada área donde se traten datos personales, dichas bitácoras contienen la siguiente información.

Anexo, Bitácora de Vulneraciones de Datos Personales

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

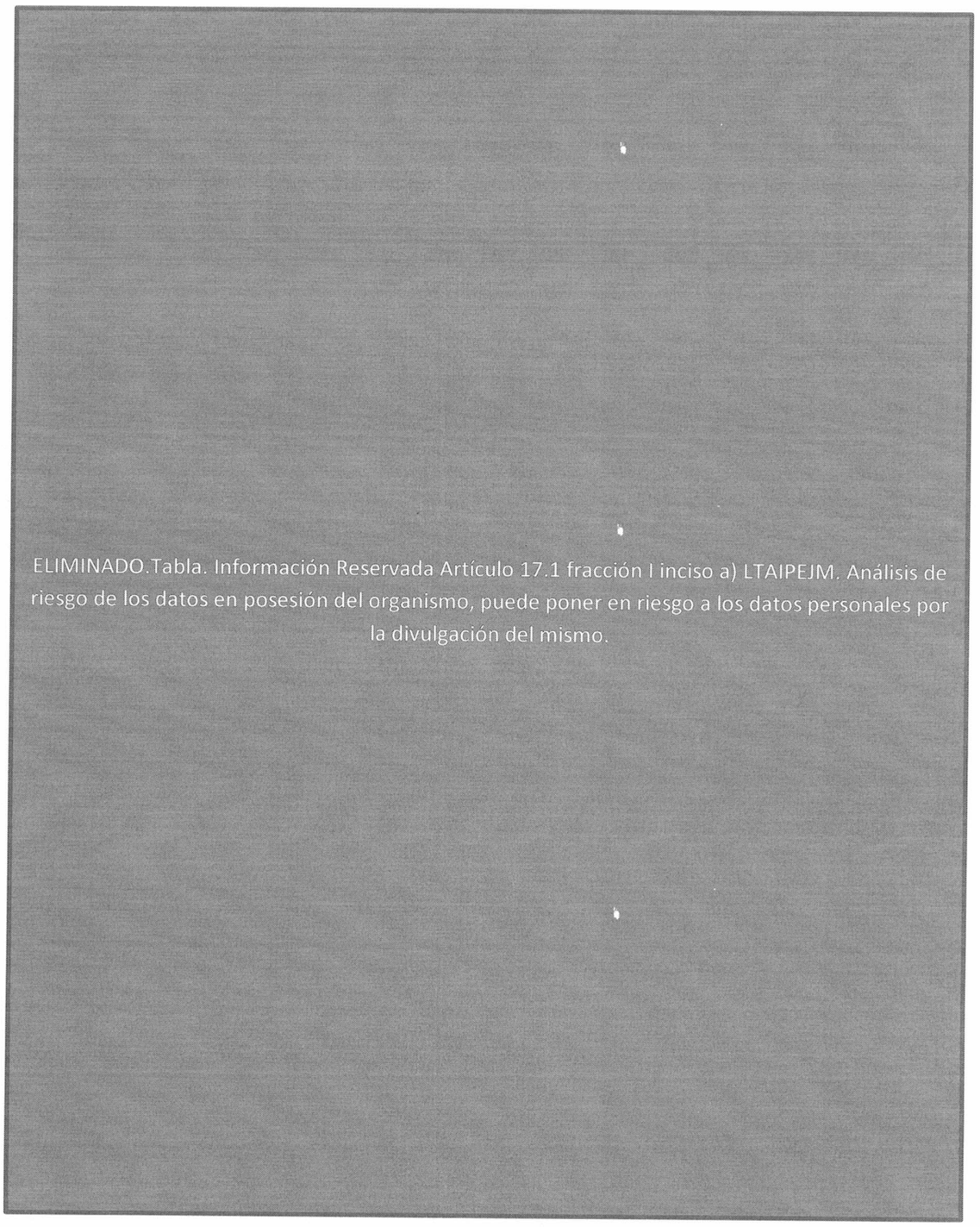
Análisis de riesgos

La Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios distingue en su artículo 38 las siguientes vulneraciones de seguridad de la información confidencial:

ELIMINADO. Información Reservada Artículo 17.1 fracción I inciso a) LTAIPEJM. Análisis de riesgo de los datos en posesión del organismo, puede poner en riesgo a los datos personales por la divulgación del mismo.

ELIMINADO. Información Reservada Artículo 17.1 fracción I inciso a) LTAIPEJM. Análisis de riesgo de los datos en posesión del organismo, puede poner en riesgo a los datos personales por la divulgación del mismo.

ORIGEN DE LA AMENAZA	CAUSA	POSIBLES CONSECUENCIAS
ELIMINADO.Tabla. Información Reservada Artículo 17.1 fracción I inciso a) LTAIPEJM. Análisis de riesgo de los datos en posesión del organismo, puede poner en riesgo a los datos personales por la divulgación del mismo.		


ELIMINADO.Tabla. Información Reservada Artículo 17.1 fracción I inciso a) LTAIPEJM. Análisis de riesgo de los datos en posesión del organismo, puede poner en riesgo a los datos personales por la divulgación del mismo.

ELIMINADO. Continuación de Tabla. Información Reservada Artículo 17.1 fracción I inciso a) LTAIPEJM. Análisis de riesgo de los datos en posesión del organismo, puede poner en riesgo a los datos personales por la divulgación del mismo.

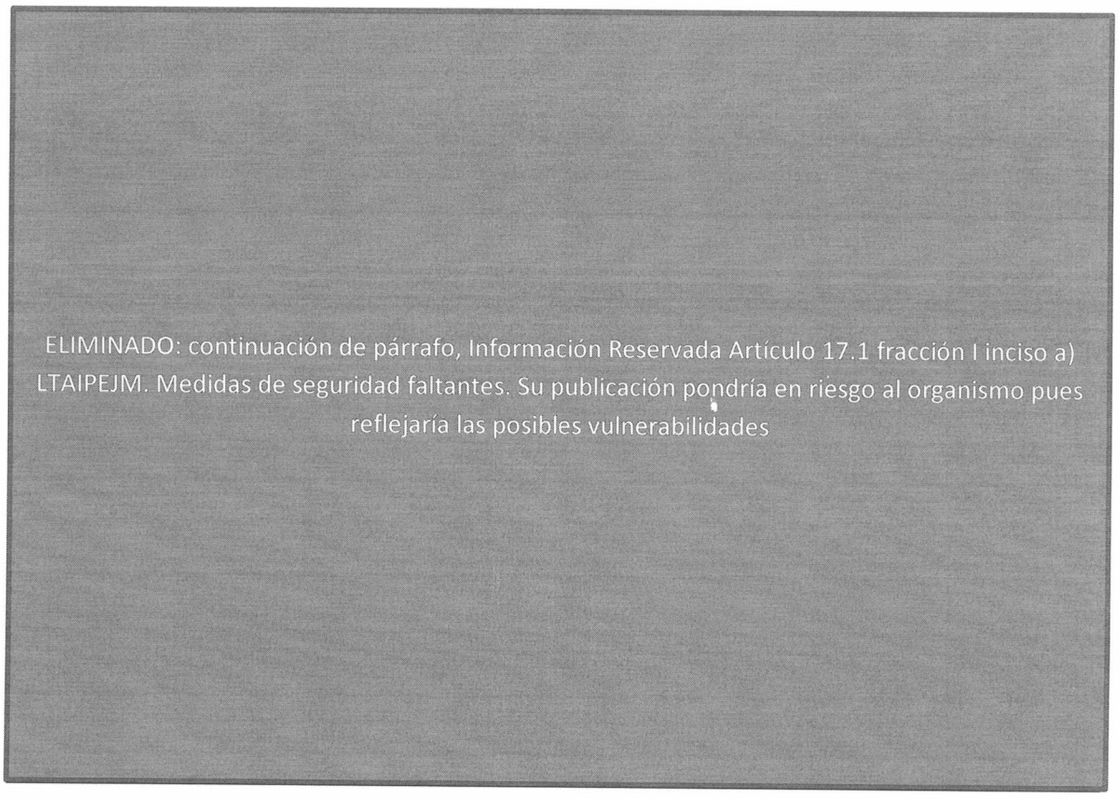
Análisis de Brecha

Una vez identificados los posibles riesgos a los que este Sujeto Obligado se encuentra susceptible de enfrentar, podemos realizar el análisis de brecha, utilizando como base los inventarios de datos personales que se hicieron con cada área.

Las diferentes direcciones reportaron las siguientes medidas de seguridad existentes:

Anexo tabla

TEMA	ESTADO ACTUAL	PARÁMETRO
ELIMINADO: párrafo, Información Reservada Artículo 17.1 fracción I inciso a) LTAIPEJM. Medidas de seguridad faltantes. Su publicación pondría en riesgo al organismo pues reflejaría las posibles vulnerabilidades		



La gestión de vulneraciones

Plan de respuesta

- Restauración Inmediata de la operatividad mediante los respaldos de los soportes electrónicos y versiones digitales de los soportes físicos;
- El personal que detecte la vulneración deberá proceder al reportar las Vulneraciones a los Sistemas de Información y Bases de Datos
- Determinación de la magnitud de la afectación y elaboración de recomendaciones para los titulares.
- Notificación a titulares en un lapso de 72 horas que de forma significativa vean afectados sus derechos.
- En caso de que la vulneración fuera resultado de la comisión de un delito se presentarán las denuncias correspondientes ante las autoridades competentes, a través de la Dirección Jurídica del organismo.

Anexo tabla

FLUJOGRAMA	DETALLE NARRATIVO

Inicio 	Se presenta contingencia en el área
El área se percata de lo sucedido	El área detecta que existe una vulneración en las bases de datos que contienen datos personales. La vulneración puede ser ocasionada por el daño, pérdida, alteración, destrucción o uso, acceso o tratamiento no autorizado de los datos personales.
El área registra evento en bitácora de vulneraciones	El encargado de la bitácora de vulneración del área registra los siguientes datos: • Fecha en que ocurrió la vulneración. • Motivo de la vulneración. • Datos personales comprometidos. • Acciones correctivas implementadas • Medidas a adoptar por el titular de los datos para proteges sus intereses. • Nombre y cargo de quién lo reporta. • Firma de quién reporta.

El área notifica a la Unidad de Transparencia sobre la eventualidad	Después del registro, se deberá informar por escrito, anexando la bitácora de vulneraciones al titular de la Unidad de Transparencia sobre las vulneraciones de seguridad ocurridas, las que afecten o impacten de forma significativa los derechos patrimoniales o morales del titular; lo anterior en un plazo máximo de setenta y dos horas.
La UT registra en formato el evento	Registra el anexo 6 y envía al ITEI los pormenores del evento de vulneración.
La UT notifica mediante oficio al ITEI anexando el formato 6	Envía al ITEI por oficio la notificación del evento de vulneración, anexando el anexo 6.

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

MEDIDAS DE SEGURIDAD IMPLEMENTADAS

Medidas de Seguridad Física:

La seguridad física consiste en la aplicación de barreras físicas, y procedimientos de control como medidas de prevención y contra medidas ante amenazas a los recursos y la información confidencial, se refiere a los controles y mecanismos de seguridad dentro y alrededor de la obligación física de los sistemas informáticos, así como los medios de acceso remoto al y desde el mismo, implementados para proteger el hardware y medios de almacenamiento de datos.

Entorno Institucional:

- Se cuenta con elementos de seguridad en la entrada del Complejo;
- Se cuenta con cámaras de video vigilancia por fuera y dentro de las instalaciones del COESIDA.
- Acceso con Gafete institucional

Entorno de los datos:

- No se sitúan equipos en sitios altos para evitar caídas,
- No se colocan elementos móviles sobre los equipos para evitar que caigan sobre ellos,
- Se separan los equipos de las ventanas para evitar que caigan por ellas o qué objetos lanzados desde el exterior los dañen,
- Colocar los equipos sobre plataformas de goma para que esta absorba las vibraciones,
- El COESIDA está provisto de equipo para la extinción de incendios conforme a lo determinado por un proveedor externo certificado.

Anexo, Tabla de Medidas de Seguridad

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

MEDIDAS DE SEGURIDAD ESTABLECIDAS POR LA UNIDAD DE TRANSPARENCIA

Administrativas	Uso de las bitácoras: • Control de acceso • Transferencias • Vulneraciones Revisiones semestrales a las áreas para comprobar el grado de apego a lo establecido en el documento de seguridad. Carta compromiso de confidencialidad del manejo de datos personales, firmada por el personal de nuevo ingreso. Constancia y acuse de recibo para transferencia de documentos físicos. Constancia para transferencia de documentos electrónicos. Se capacita al personal que trabajan con datos personales por lo menos una vez al año, se cuentan con 3 capacitaciones al año en diferentes temas, se va capacitando al personal específico de los temas impartidos
Físicas	Eliminación y entrega de los medios de almacenamiento: Los medios deberán eliminarse de modo seguro cuando no se les necesite más, usando procedimientos formales Los expedientes físicos y electrónicos que contienen datos personales no se tienen al alcance de cualquier persona. Prevenir el acceso no autorizado a la Coordinación General Estratégica de Seguridad y Secretaría de Seguridad, sus instalaciones físicas, áreas críticas, recursos e información. Se cuentan con procedimientos y medidas de seguridad recomendadas y aplicables por Protección Civil al interior de las instalaciones. Proteger los Recursos móviles, portatiles y cualquier soporte físico o electrónico que pueda salir de la Coordinación General Estratégica de Seguridad y Secretaría de Seguridad. Se cuentan con mecanismos y acciones que permiten identificar los equipos móviles y portátiles: mobiliario, documentos y materiales mediante controles de entrada y salida, tales como: control en el ingreso y egreso de aparatos, equipos, mobiliarios, documentos y materiales mediante la autorización por los titulares de las áreas.

	En la mayoría de las áreas, el acceso (al área donde se recibe a los ciudadanos y se recaban datos personales) se tiene restringido, una vez que el dato se encuentra en posesión del servidor público, es decir si fue recabado frente a un escritorio, área abierta o pasillo, los ciudadanos no podrán pasar detrás de estos, ya que al terminar de recabar datos estos se colocan fuera del alcance de los ciudadanos. La oficina cuenta con puertas que cierra el área al momento de terminar labores. Las llaves que se tienen de la oficina se encuentran en manos de servidores públicos, autorizados por el área general. Cada carpeta de trámites o archivo, al terminar el proceso de cada uno, son resguardados en un archivo de cada área. El aviso de privacidad se encuentra a la vista y alcance de los ciudadanos, es decir en el espacio físico donde se recaban los datos personales.
Técnicas	El acceso a las bases de datos es exclusivo para aquellos cuyas áreas o unidades responsables de la información han autorizado. Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware. Las áreas son responsables de validar el perfil del usuario que se apegue a lo necesario, para cumplir con las funciones de los sistemas de información, las áreas son responsables de los procesos respectivos. Respaldos semanales por parte del área de informática.

Procedimientos de respaldo y recuperación de datos personales

Respaldo Se realiza una digitalización completa de la información por parte de cada área responsable y se almacena en discos duros. A partir de la aprobación del presente documento deberá realizarse un respaldo incremental almacenado en discos duros. -Una operación de respaldo incremental sólo copia los datos que han variado desde la última operación de respaldo de cualquier tipo.

Cada área será la responsable de almacenar sus respaldos durante el tiempo que señale el catálogo de disposición documental del COESIDA.

Recuperación. - Los respaldos incrementales contienen fecha y hora, tanto inicial como final. La recuperación se realiza cruzando la fecha del incidente y el último respaldo.

Anexo, Bitácora de Transferencias de Datos Personales

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

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

Bitácora de Acceso a los Datos Personales

La bitácora de acceso a los datos personales se utiliza sólo en los casos de que se trate de expedientes físicos y contienen la siguiente información:

- Nombre y cargo de quien accede
- Identificación del Expediente
- Fojas del Expediente
- Propósito del Acceso
- Fecha de Acceso
- Hora de Acceso
- Fecha de Devolución
- Hora de Devolución

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

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

Plan de Contingencia

Ante la pérdida total o parcial de datos personales en posesión de este sujeto obligado, se debe contar con un plan de contingencia, que nos permita dar continuidad a la aplicación de este documento de seguridad, así como enfrentarnos a fallas y eventos inesperados que podrían derivar en la pérdida parcial o total de la información confidencial que posee este sujeto obligado.

Con la evaluación de riesgos y la elaboración de las medidas de seguridad aplicables para prevenir las posibles vulneraciones y daños a los que nos encontramos expuestos, nos

encontramos con que el plan de contingencias de este sujeto obligado consiste en la aplicación de las medidas de seguridad tratadas en el apartado anterior, mismas que están sujetas a cambios por eventualidades no contempladas, por ello la importancia de señalar que el presente se trata de un plan de contingencia no limitativo.

Lo anterior toda vez que en la actualidad existen cambios y grandes avances que van modificando la organización de la información, y al igual existen riesgos inminentes que día a día evoluciona.

En caso de cualquier vulneración o daño a la seguridad de los datos personales, se deberá actuar con eficiencia, de forma rápida y oportuna, así como en todo momento procurar minimizar el daño, asegurando tener las menores pérdidas posibles y buscando la mayor recuperación de la información en el menor tiempo y costo posible para la dependencia.

En caso de que los datos personales sufran algún tipo de daño o pérdida, se dispondrá de los respaldos electrónicos realizados por cada dirección en donde se contienen copias de documentos y/o archivos y/o bases de datos que contienen datos personales que permitirían restablecer los datos a la fecha del último respaldo.

Clasificación de las emergencias

Las situaciones de emergencia pueden presentarse en cualquier momento derivado de un accidente o incidente grave. Cada emergencia requiere de una adecuada respuesta de acuerdo a la gravedad de la situación, para ello se definen tres niveles:

Emergencia de grado 1: Comprende la afectación de un área de operación y puede ser controlada con los recursos humanos y equipos de dicha área.

Emergencia de grado 2: Comprende aquellas emergencias que por sus características requieren de recursos internos y externos.

Emergencia de grado 3: Comprende aquellas emergencias que, por sus características, magnitud y alcances, requieren de recursos internos y externos.

Consideraciones Principales

- Se debe realizar una evaluación de los riesgos.
- Dentro de la implementación del plan de contingencia se debe contar con un responsable general quien guiará la implementación del mismo, así como la toma de las decisiones.
- Se designe a un encargado de cada área para que apoye en cualquier desastre que ocurra y genere la contingencia, capacitándolos para el manejo de las mismas, como el uso de extintores, planes de evacuación etc.
- Es necesario hacer las pruebas previas del plan de contingencia para garantizar su funcionalidad en caso de siniestro (las pruebas generalmente se hacen en tiempo real y lo más aproximados a la realidad).
- Reunión con las comisiones o brigadas (capacitación y evaluaciones)

- Revisión del Plan e integración de las recomendaciones y decisiones adoptadas de acuerdo con las lecciones aprendidas del ejercicio.
- Difusión del documento del plan de contingencia una vez aprobado.
-

Lugar alternativo de trabajo

En caso de algún desastre mayor (terremoto o incendio) que implique perdidas estructurales se plantea en algunos casos la posibilidad de contar con algún lugar alternativo de trabajo los sitios alternos de trabajo pueden ser: propios de la organización, de una entidad con la que hay acuerdo o reciprocidad, instalaciones alquiladas.

En caso de contar con un ambiente alterno debe contar con los siguientes recursos:

• Mesas para monitores y teclados de los servidores principales

• Sillas

• Switches

• Router para la conexión a internet

• UPS

• Teléfono

• Extinguidor

• Útiles de Oficina

Medidas preventivas ante siniestros

Medidas de prevención y conservación de archivos

- A los archivos de las áreas solo deben de tener acceso las personas responsables, para evitar algún robo, destrucción o alteración del archivo.
- Debe contar con luz natural, sin que le dé directamente el sol.
- Espacios libres de humedad.
- Mantener el archivo limpio para evitar el polvo y la contaminación.
- No debe de haber archivos directamente con el suelo, mantenerlo entre 10 y 15 cm.
- Proteger los equipos eléctricos manteniéndolos en buenas condiciones y con las medidas de protección adecuadas.
- Evitar alimentos cercas de los archivos y bebidas que puedan derramarse sobre aparatos eléctricos.
- Los aparatos eléctricos que no se utilicen deberán de estar apagados o desconectadas.

Incendios

Medidas preventivas en caso de incendio:

- Conocer el plan de evacuación.
- Es recomendable saber lo básico de primeros auxilios.
- Identificar las salidas de emergencias.
- Contar con alarma o silbato para que puedan darse cuenta y proceder a evacuar correctamente.
- No contar con sustancias inflamables (tiner, gasolina, alcohol, aceite, acetona) en caso de tenerlos, alejarlos de flamas y resguardarlos en lugares apartados que puedan ocasionar incendios.
- Instalar el equipo adecuado en zonas específicas.
- Si el incendio es pequeño apagarlo con el extintor.
- No sobrecargar los contactos eléctricos, de preferencia contar con reguladores de energía para evitar una sobrecarga.
- No apagar incendios si son de origen eléctrico.

Sobre el resguardo de la información en caso de incendio:

- Respaldo de los archivos en zonas seguras o donde se pueda reaccionar de manera inmediata para contener el fuego.
- Tener identificados los documentos de mayor valor para resguardarlos en zonas seguras.
- Se pueden asegurar los documentos en CD, USB, Disco duro, caja de seguridad y resguardo en la nube si es segura.

Durante un incendio:

- Guarda la calma.
- Dar una señal de alarma de incendio.
- Evalúa la situación, trata de ver que se quema, en qué cantidad, el sitio donde está el fuego y si éste puede propagarse.
- Si sabe usar los extintores cerciorarse de que pueda usarlos y que funcionen.
- Si es un incendio que no se pueda controlar llamar inmediatamente a los bomberos.
- Trata de controlar la situación retirando a las personas a un lugar seguro o utilizando un extintor.
- Si el incendio tiende a propagarse evacúa el área.
- Baja por las escaleras de emergencia, no utilices los elevadores.
- Si no puedes bajar, intenta estar en una zona segura; deja abierta la puerta de acceso a la misma para que el humo no se acumule.
- No te encierres en baños u oficinas, ni te metas debajo de mesas, escritorio, etc., ya que el humo y el calor invadirán toda el área

- En caso de gas o humo humedecer un trapo o camisa y cubra boca y nariz.

Después del Incendio:

- No pases al área del siniestro hasta que las autoridades lo determinen
- Espera el diagnóstico de las autoridades y los expertos para poder ingresar
-

Terremoto

El daño ocasionado por un terremoto puede dañar principalmente la estructura del edificio, sin embargo, si los datos almacenados se encuentran en discos duros, cd, USB, al contar con un respaldo de información incluso en la nube se tiene un respaldo inmediato, que permitiría recuperar la información si los otros respaldos físicos se dañaran, para inmediatamente apenas se tenga una conexión a internet y una computadora tener acceso a dichos respaldos.

Medidas preventivas en caso de sismo

- Tenga a la mano números telefónicos de emergencia, botiquín, de ser posible un radio portátil y una linterna con pilas.
- Contar con un botiquín de emergencia
- Ubicar los lugares seguros si no se puede salir rápidamente: mesas, escritorio, paredes.
- Identificar los lugares peligros: ventadas, aparatos que puedan caerse, lámparas, etc.
- Identifique los lugares más seguros de inmueble, las salidas principales y alternas.
- Contar con teléfono celular de emergencia en caso de fallar las líneas telefónicas fijas.
- Hacer simulacros de emergencia.
- Verifique que las salidas y pasillos de emergencia se encuentren sin obstáculos.

Durante un sismo

- Conserve la calma, no permita que el pánico se apodere de usted.
- Diríjase a los lugares seguros previamente establecidos; cúbrase la cabeza con ambas manos colocándola junco a las rodillas.
- No utilice los elevadores.

- Aléjese de los objetos que puedan caer, deslizarse o quebrarse.
- Alejarse de las ventanas y objetos de vidrio.
- No se apresure a salir, el sismo dura sólo unos segundos y es posible que termine antes de que usted lo haya logrado.
- De ser posible tome las medidas necesarias para evitar un incendio.

Después de un Sismo:

- En caso de quedar atrapado, conserve la calma y trate de comunicarse con el exterior
- Usar el teléfono solo para emergencias
- Mantenerse alejado de las áreas de desastre.
- En caso de que la estructura fue dañada evitar regresar, ya que después vienen las réplicas.
- No encender flamas o cualquier cosa que pueda provocar un incendio.
- Hasta que la situación sea evaluada y las autoridades correspondientes den autorización de entrar al edificio se puede entrar.

Inundaciones por lluvia

Durante la temporada de lluvias se presentan algunas circunstancias que provocan encharcamientos, inundaciones o fugas en vialidades; lo anterior tiene como origen, entre otros, la saturación del drenaje y escurrimientos de agua hacia partes bajas de la zona, lo que provoca marcas sobre materiales porosos, protuberancia de materiales orgánicos, oxidación de metales, roturas y desprendimiento de papel.

Medidas preventivas en caso de inundación

- Cambiar el recorrido de los sistemas de tuberías que pasan directamente por encima de
- los archivos.
- Revisión y reparación de las ventanas y puertas por donde puede filtrarse el agua de lluvia.
- Levantamiento de desniveles en pisos y suelos a los que pueda llegar agua de inundación, por derrames incontrolados, sumideros o desagües conducidos a la red de alcantarillado.
- Que la ubicación de las válvulas de control de flujo (llave de paso), sea ampliamente conocida por el personal.

- Evitar en lo posible colocar expedientes y/o documentos directamente sobre el piso.

Durante una inundación

- Desconectar servicios de luz, gas y agua.
- Mantenerse alejados de árboles y postes de luz.
- Evitar tocar o pisar cables eléctricos.
- Colocar barreras para el agua (cubrir los documentos con plásticos, cubetas o recipientes para las goteras) en la parte superior de los estantes dentro del local de archivo.
- buscar lugares altos para mantenerse fuera de peligro.
- Cubrir con bolsas de plástico aparatos u objetos que puedan dañarse con el agua.

Después de la inundación

- Evacuar los documentos afectados hacia áreas ventiladas.
- Desinfectar las áreas afectadas pisos, muros y mobiliario rescatable, con agua, jabón y cloro para evitar enfermedades.
- Si el riesgo de acumulación de agua lo merece, expulsar el agua con una bomba de achique con motor de combustión o eléctrico, si hay suministro eléctrico garantizado en caso de emergencia, y si no hubiere, mediante esponjas, baldes, recogedores, etc.
- Si se interviene de inmediato, se colocará papel secante en cada hoja de los expedientes.
- Si la documentación está húmeda al 100% se debe proceder a su congelación. El procedimiento de rescate es muy largo y delicado, debe realizarlo preferentemente un especialista (restauración).
- Los documentos mojados serán extendidos sobre mesas o anaqueles para su secado por ventilación natural y/o artificial. No debiendo exponerse al calor, ni de manera directa a los rayos solares

Robo

Robo Común de equipos:

En caso de robo a mano armada se sugiere contar con teléfonos de emergencia de diferentes dependencias.

Amenazas informáticas

Medidas preventivas para amenazas informáticas

- Es necesario contar con un inventario actualizado de los equipos de cómputo, impresoras, escáner, fotocopiadoras etc., y tener contacto con proveedores de software, hardware, y medios de soporte.
- Prevención de falla de los equipos: se debe procurar dar mantenimiento preventivo por lo menos una vez al año, y contar con proveedores en caso de que se requiera algún remplazo inmediato.
- Los equipos pueden quedar dañados por fallas eléctricas, se requiere contar con estabilizadores /reguladores, en cada uno de los equipos principalmente en aquellos que su afectación implique la perdida de información importante.

Hackeo informático:

Ante un evento de hackeo informático los pasos a seguir para mantener la seguridad de la información, son los siguientes:

Cambiar contraseñas.

- Debe tener al menos ocho caracteres
- No debe contener información personal como nombre real, nombre de usuario
- Debe ser muy distinta a tus contraseñas previas

No debe contener palabras completas

Debe contener caracteres de las cuatro categorías primarias: mayúsculas, minúsculas, números y caracteres especiales

Mientras se está conectado a Internet el Hacker tendrá acceso a los archivos e información guardados en la computadora hackeada.

Por lo que se debe **desconectar el cable de la red lo antes posible.**

Posteriormente:

Contactar al personal de soporte para que retire del aire la página.

Evalúe los daños causados: El experto debe evaluar qué información se perdió y cuál es la que se mantiene para restaurar el sitio lo antes posible.

Mantener la misma dirección web

Cuando la página fue atacada la dirección usualmente no se ve afectada. Lo que generalmente se pierde es la información (textos, videos, fotos, audios) que contenía. Se sugiere restaurar el sitio con la misma dirección, para que los usuarios no se confundan.

Técnicas de Supresión y Borrado Seguro de Datos Personales

Métodos Físicos

1. **Trituración mediante corte horizontal**: Cortar el documento de forma horizontal generando fragmentos diminutos, lo cual hace prácticamente imposible que se puedan unir.
2. **Destrucción de los medios de almacenamiento electrónicos** mediante desintegración, consistente en separación completa o pérdida de la unión de los elementos que conforman algo.

Métodos Lógicos

Sobre-escritura: consiste en sobrescribir todas las ubicaciones de almacenamiento utilizables en un medio de almacenamiento, es decir, se trata de escribir información nueva en la superficie de almacenamiento, en el mismo lugar que los datos existentes, utilizando herramientas de software.

Plan de trabajo

La existencia del documento de seguridad, busca enmarcar los deberes, para la óptima protección de datos personales; en ese sentido, debido a la importancia en materia de datos personales, se debe mantener actualizado el plan de trabajo, el cual permita alcanzar los objetivos del sistema de seguridad.

Con base en lo anterior, se ha planteado implementar la totalidad de las medidas de seguridad faltantes en un periodo de seis meses a partir de la aprobación del presente documento de seguridad; con base en lo anterior, las medidas de seguridad físicas y técnicas que requieran la erogación de recursos, se realizarán conforme a los tiempos administrativos y el presupuesto lo permita.

Para la ejecución del presente documento de seguridad, se dará prioridad a las siguientes actividades:

Mes 1 a 3

1. Se informará y difundirá el documento de seguridad, a través los correos institucionales.
2. Se comenzara con la capacitación los servidores públicos que recaban datos personales;

Mes 3 a 6

1. Se verificación de vigencia de los sistemas de información y el cumplimiento de los estándares de seguridad;

Los mecanismos de monitoreo y Revisión de las medidas de seguridad

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

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

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

Programa General de Capacitación

La capacitación del personal del COESIDA es anual y con las siguientes temáticas:

Tema	**Tipo de Capacitación**
Generalidades de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios	Sesión Informativa
Protección de Datos Personales en Salud	Sesión Informativa
Medidas de seguridad para la Protección de Datos personales en salud	Taller