DOCUMENTO DE SEGURIDAD

INEEJAD

Instituto Estatal para la Educación de Jóvenes y Adultos

El presente documento contiene las disposiciones en materia de protección de datos personales de las unidades administrativas de este Instituto Estatal para la Educación de Jóvenes y Adultos.

J. Guadalupe Zuno 2091
Col. Deitz
Guadalajara, Jalisco, México
C.P. 44158
01 (33) 3030 4350

#AprenderTeTransforma
INEEJAD Oficial @INEEJAD_OFICIAL

Introducción

En la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios se establecen las bases, principios, procedimientos y tratamiento que permite garantizar la protección de datos personales de los ciudadanos en posesión de este Instituto Estatal para la Educación de Jóvenes y Adultos (INEEJAD) como sujeto obligado.

Teniendo como base dicha normatividad, se crea el presente documento de seguridad ya que en el Instituto Estatal para la Educación de Jóvenes y Adultos (INEEJAD), la información es un activo que debe protegerse mediante un conjunto coherente de procesos y sistemas diseñados, administrados y mantenidos por el mismo. De esta manera, la gestión de la seguridad de la información, como parte de un sistema administrativo más amplio, busca establecer, implementar, operar, monitorear y mejorar los procesos y sistemas relativos a la confidencialidad, integridad y disponibilidad de los datos personales, aplicando un enfoque basado en los riesgos que el Instituto afronta.

El presente Documento de Seguridad para Sistemas de Datos Personales en medios físicos (Documento), se dicta en cumplimiento de las disposiciones jurídicas vigentes, para la mejor protección de los sistemas registrados en el INAI, con el fin de asegurar la integridad, confidencialidad y disponibilidad de la información personal que éstos contienen.

El Documento brinda al Instituto 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 y física implementadas para la protección de los sistemas de datos personales custodiados.

Así mismo, este documento tiene como propósito controlar internamente el universo de sistemas de datos personales que posee el Instituto, el tipo de datos personales que contiene cada uno, los responsables, encargados, usuarios de cada sistema y las medidas de seguridad concretas implementadas.

Glosario
Medidas de seguridad implementadas
Procedimientos de respaldo y recuperación de datos personales
Controles y mecanismos de seguridad para las transferencias
Bitácoras de Acceso, Operación Cotidiana y Vulneraciones a la Seguridad de los Datos Personales
Controles de Identificación y Autenticación de Usuarios
Técnicas de Supresión y Borrado Seguro de Datos Personales
Análisis de riesgos
Identificación de Medidas de Seguridad
Gestión de vulneraciones
Plan de respuesta
Mecanismos de monitoreo y revisión de las medidas de seguridad
Análisis de brecha
Plan de trabajo
Programa General de Capacitación
Plan de Contingencia
Catálogo de Sistemas de Tratamiento de Datos Personales

Glosario

Bases de datos	Conjunto ordenado de datos personales referentes a una persona física identificada o identificable, condicionado a criterios determinados con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.
Disociación	El procedimiento mediante el cual los datos personales no pueden asociarse al titular ni permitir, por su estructura, contenido o grado de desagregación, la identificación del mismo.
DMZ	En seguridad informática, una zona desmilitarizada (conocida también como DMZ, sigla en inglés de *demilitarized zone*) o red perimetral es una zona insegura que se ubica entre la red interna de una organización y una red externa, generalmente en Internet. El objetivo de una DMZ es que las conexiones desde la red interna y la externa a la DMZ estén permitidas, mientras que en general las conexiones desde la DMZ solo se permitan a la red externa -- los equipos (*hosts*) en la DMZ no pueden conectar con la red interna. Esto permite que los equipos (*hosts*) de la DMZ puedan dar servicios a la red externa a la vez que protegen la red interna en el caso de que intrusos comprometan la seguridad de los equipos (*host*) situados en la zona desmilitarizada. Para cualquiera de la red externa que quiera conectarse ilegalmente a la red interna, la zona desmilitarizada se convierte en un callejón sin salida
DNS	Un Servidor DNS en informática responde a las siglas *Domain Name System*. Gracias a los servidores DNS

	conocemos los nombres en las redes, como las de Internet o las de una red privada.
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.
INAI	Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.
Instituto	Instituto Estatal para la Educación de Jóvenes y Adultos.
ITEI	Instituto de Transparencia, Información Pública y Protección de Datos Personales del Estado de Jalisco.
LAN	Una red de área local o LAN (por las siglas en inglés de *Local Area Network*) es una red de computadoras que abarca un área reducida a una casa, un departamento o un edificio.
Ley	Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios.

Ley de Transparencia	Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios.
Ley General	Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados
Ley General de Transparencia	Ley General de Transparencia y Acceso a la Información Pública
Medidas de seguridad	Conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permiten garantizar los protección, confidencialidad, disponibilidad e integridad de los datos personales.
Medidas de seguridad administrativas	Políticas y procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, la identificación, clasificación y borrado seguro de la información, así como la sensibilización, formación y capacitación del personal en materia de protección de datos personales.
Medidas de seguridad físicas	Conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento.
Medidas de seguridad técnicas	Conjunto de acciones y mecanismos que se valen de la tecnología relacionada con hardware y software para proteger el entorno digital de los datos personales y recursos involucrados en su tratamiento.
N/A	No aplica.
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 son 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.

Medidas de seguridad implementadas

Medidas de Seguridad Físicas

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.

- Quien recaba los datos personales, es un servidor público del área, asignado especialmente para recabar datos en general necesarios para cada trámite.

- El espacio físico o área donde se recaban datos personales, es dentro de las instalaciones.

- Cuando los datos personales son recabados de forma digital, se realiza por medio de plataformas oficiales o correo electrónico oficial.
- 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, ventanilla, 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.
- Los accesos a cada área se encuentran en manos de servidores públicos, autorizados
- Una vez recabados los datos personales, el servidor público genera un expediente para cada trámite o servicio, del cual se obtuvieron los datos personales, ya sea físico o electrónico.
- Una vez recabados los datos personales, en caso de que se les dé proceso electrónico, el servidor público guarda los mismos en carpeta electrónica, ya sea en su computadora, correo electrónico oficial o plataforma.
- Durante el desahogo del trámite del cual se obtuvieron los datos personales, los servidores públicos del área tienen acceso a los datos personales.
- Una vez concluido el trámite, los datos personales recabados se dejan intactos en la carpeta, archivo o expediente del trámite al que pertenecen.
- 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.
- El servidor público que reciba los datos personales, deberá tener a la vista de todos los ciudadanos el aviso de privacidad, y darlo a conocer al momento de la recepción del trámite.
- Si el trámite del cual se recabarán datos personales, cuenta con un formato, este deberá contener la mención y debe dar a conocer el aviso de privacidad del Instituto, ya sea simplificado o la liga de internet que remita al ciudadano al aviso general. Los formatos nuevos que se impriman posteriores a la emisión del presente documento deberán contar con la liga al aviso de privacidad o en su defecto el aviso de privacidad simplificado.
- Para evitar riesgos, respecto a los expedientes electrónicos, se debe contar con un respaldo electrónico. Dicho respaldo deberá realizarse, como mínimo, de manera anual.

- Cada área del sujeto obligado deberá elaborar controles de archivo, conforme a sus procesos institucionales. Esto es, un inventario de documentos el cual se tiene por obligación vinculada con la armonización que la Ley General de Transparencia y Acceso a la Información Pública dispone en sus artículo 24 fracción IV y 70 fracción XLV.

Medidas de seguridad para transferencias:

Solo podrán ser transferidos los datos personales para dar seguimiento y conclusión al trámite o sistema de tratamiento bajo la finalidad que éstos prevean, al interior del sujeto obligado y a otros sujetos obligados.

- El área que entrega los datos personales deberá cerciorarse de transferir la totalidad de los datos que resulten necesarios para el seguimiento o la conclusión del trámite o sistema de tratamiento correspondiente. Limitándose a la entrega de datos adicionales que no resulten necesarios.

- El área que entrega los datos personales deberá cerciorarse de que los datos que transfiere sean completos y veraces.

- El área que reciba los datos personales deberá conservar los mismos sujetándose a las finalidades y lineamientos del aviso de privacidad de este sujeto obligado y adoptando las medidas de seguridad previstas en este documento.

- El área que reciba los datos personales deberá encargarse de la supresión de los datos que reciba cuando esta corresponda.

- El área que entrega y el área que recibe los datos personales deberán dar acceso a los datos personales tratándose de procedimientos de derecho ARCO.

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

En caso de ser necesario conforme a las disposiciones normativas, se deberá firmar un convenio o acuerdo de confidencialidad que proteja el tratamiento de los datos personales que recaba este sujeto obligado y transfiere al tercero.

Medidas de seguridad en caso de vulneraciones a la seguridad:

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 y anexar a su plan de trabajo las 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 ante el Órgano de Control Interno.

Medidas de seguridad o controles para la identificación y autentificación de usuarios:

El Instituto Estatal para la Educación de Jóvenes y Adultos (INEEJAD), con la finalidad de tener un control efectivo al trato de los datos personales dispone lo siguiente:

1. Los empleados (Federales y Estatales) deben portar en todo momento su identificación institucional que cuenta con la siguiente información en la parte frontal: (fotografía, nombre, área de adscripción y cargo) en la parte posterior (Id de empleado, CURP, nombramiento, No. de Seguro Social, tipo de sangre, teléfono de emergencia y fotografía)

2. Cuentas de usuario, parte esencial de los sistemas que se desarrollan en el departamento de informática de este Instituto, razón que verificar la identidad de cada funcionario. (Esta medida es tomada para los correos electrónicos institucionales, computadoras ya que precisan de un nombre de usuario y contraseña para ingresar y para cualquier sistema o plataforma tecnológica que creé este sujeto obligado)

Procedimientos de respaldo y recuperación de datos personales

A partir de la aprobación del presente documento, se realizará una digitalización anual completa de la información que ingresa y deberá generarse un respaldo incremental almacenado en discos duros. (La copia incremental, es la más avanzada al respecto, ya que únicamente copia los ficheros creados o modificados desde el último backup realizado, ya sea de una copia completa o incremental, reduciendo de este modo los archivos a copiar y el tiempo empleado en el proceso de backup)

Cada área será la responsable de almacenar sus respaldos durante el tiempo que se señale.

En lo que respecta a la recuperación, los respaldos incrementales contienen fecha y hora, tanto inicial como final, por lo que la misma se realiza cruzando la fecha del hecho y el último respaldo.

Bitácoras de Acceso, Operación Cotidiana y Vulneraciones a la Seguridad de los Datos Personales

Bitácoras de Acceso	1. Las bitácoras de acceso a los datos personales se utilizan en los soportes físicos y contienen la siguiente información: • Nombre y cargo de quien accede • Identificación del Expediente • Fojas del Expediente • Propósito del Acceso • Fecha de Acceso • Fecha y hora de Devolución 2. Las bitácoras se encuentran en soporte físico 3. Son resguardadas por los titulares de cada área en el lugar que para tal efecto designen.

Bitácoras de Vulneraciones a la Seguridad de los Datos Personales	La bitácora de vulneraciones contiene la siguiente información 1. Nombre del responsable de la investigación 2. Cargo 3. Área 4. Número de investigación 5. Sistema (s) de información o base (s) de dato (s) vulnerado (s) 6. Tipo de vulneración 7. Tipo de datos personales comprometidos

	8. Nombre y firma de quien reporta 9. Nombre y firma del administrador del sistema 10. Nombre y firma del titular del área

Técnicas de Supresión y Borrado Seguro de Datos Personales

Trituración mediante corte cruzado o en partículas: Cortar el documento de forma vertical y horizontal generando fragmentos diminutos, denominados "partículas", lo cual hace prácticamente imposible que se puedan unir.

Sobrescribir todas las ubicaciones de almacenamiento utilizables en un medio de almacenamiento, es decir, escribir información nueva en la superficie de almacenamiento, en el mismo lugar que los datos existentes, utilizando software acorde.

Análisis de riesgos

Debido a las circunstancias generales, tanto físicas como humanas, en las que se tratan datos personales, se identificaron los siguientes posibles riesgos:

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

Identificación de Medidas de Seguridad

Las medidas de seguridad que actualmente se llevan a cabo pudieran ser efectivas de aplicarse de manera continua y consciente en las áreas administrativas de este sujeto obligado. El riesgo latente que se provoca por la falta de conocimiento, o compromiso para la aplicación de estas medidas existentes se puede minimizar por medio del establecimiento obligatorio de dichas medidas de seguridad y de la mejora continua de las mismas.

Por lo que a partir de la aprobación de este documento se deberá generar un listado de los servidores públicos que recaban datos personales, esto es, de los servidores públicos que tienen contacto con el titular de los datos personales por sus funciones, mismo que deberá estar en constante actualización.

Forzosa asistencia a por lo menos a 1 capacitación anual en materia de datos personales impartida por la Unidad de Transparencia de este sujeto obligado y/o la Coordinación General de Transparencia del Gobierno de Jalisco y/o el Órgano garante (ITEI).

Difusión al documento de seguridad para el conocimiento y cumplimiento de las medidas de seguridad aplicables para un correcto tratamiento de datos personales.

Para evitar el riesgo de obtener datos personales incompletos o incorrectos, el servidor público autorizado para recabarlos, deberá pedir al ciudadano acredite su personalidad.

Al finalizar el desahogo de los expedientes estos deberán archivarse en un lugar adecuado el cual no debe estar al alcance de los ciudadanos o servidores públicos ajenos al área.

En caso de ser necesario derivado de las funciones de los servidores públicos, o por requisito del trámite, se deba realizar una transferencia de datos personales, se deberá informar al sujeto que reciba los datos el aviso de privacidad para que se sujete al mismo.

En los casos en los cuales se realicen clasificaciones de información confidencial, que incluyan datos personales, los documentos que contengan los datos, deberán entregarse siempre en versión pública, adjuntando índice de datos personales.

Eliminación o reutilización segura del equipo: Todos los artículos de equipo que contengan medios de almacenamiento deberán revisarse para asegurar la remoción o sobre-escritura apropiada de cualquier información sensible y "software" de autor antes de su eliminación

Controles contra código malicioso: Se deberán implementar controles para la detección, prevención y recuperación de la infraestructura en contra de códigos maliciosos. Se deberán implementar procedimientos de concienciación adecuados.

Controles de red: Las redes deben ser gestionadas y controladas con el fin de ser protegidas de las amenazas, y para mantener la seguridad de los sistemas y aplicaciones que utilizan la red, incluyendo la información en tránsito.

Administración de privilegios: Deberá restringirse y controlarse la asignación y uso de privilegios

Uso de contraseñas: Se deberá exigir a los usuarios que sigan buenas prácticas de seguridad en la selección y uso de las contraseñas

Equipos desatendidos: Los usuarios deberán asegurar que los equipos atendidos cuenten con protección adecuada.

Identificación y autenticación de usuarios: Todos los usuarios deben tener un identificador único (ID de usuario) para su uso personal, y una técnica de autenticación adecuada debe ser elegido para fundamentar la identidad declarada de un usuario.

Control de vulnerabilidades técnicas: Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se utilizan. Se debe evaluar la exposición de la organización a las mismas y se deben tomar las medidas apropiadas para enfrentar los riesgos asociados.

Medidas de Seguridad Físicas

Eliminación de los derechos de acceso: Los derechos de acceso de todos los empleados, y usuarios de terceras partes, a información e instalaciones de procesamiento de información deben ser removidos en cuanto se termine el trabajo, contrato, acuerdo o cuando se requiera hacer un ajuste.

Perímetro de seguridad física: Control de acceso.

Medidas Reforzadas de Seguridad para Accesos desde Entornos de Alta Anonimidad

Controles de red: Las redes deben ser gestionadas y controladas con el fin de ser protegidas de las amenazas, y para mantener la seguridad de los sistemas y aplicaciones que utilizan la red, incluyendo la información en tránsito.

Uso Sistema de monitoreo: Se deben establecer procedimientos para monitorear el uso de la información y los sistemas. Los resultados de las actividades de monitoreo deben ser revisados con regularidad.

Administración de privilegios: Deberá restringirse y controlarse la asignación y uso de privilegios.

Política de uso de los servicios de red: Los usuarios sólo deben contar con acceso a los servicios para los que han sido autorizados.

Control de conexión de red: Se deberá restringir la capacidad de los usuarios para conectarse a redes compartidas.

Control de enrutamiento de la red: Los controles de enrutamiento deben aplicarse a las redes para garantizar que las conexiones informáticas.

Fuga de información: Se deben prevenir las oportunidades de fuga de información.

Control de vulnerabilidades técnicas: Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se utilizan. Se debe evaluar la exposición de la organización a las mismas y se deben tomar las medidas apropiadas para enfrentar los riesgos asociados.

Disociación de información cuando los datos pasen de un ambiente de riesgo menor a un ambiente de riesgo mayor.

Controles de DNS

Únicamente permitir servicios públicos dentro de la DMZ

Mejores prácticas de configuración del FW

Red inalámbrica conectada a la zona desmilitarizada (DMZ) externa

Red de terceros conectada a la zona desmilitarizada (DMZ) externa

Controles de tráfico entrante y saliente

Monitorear sistemas de prevención de Intrusos (IPS)

Análisis de brecha

Una vez identificados los posibles riesgos a enfrentar, podemos realizar el análisis de brecha, utilizando como base las medidas de seguridad existentes. Por lo que de aplicarse de manera continua y consciente en las áreas las mismas resultarían efectivas. No obstante, el riesgo que provoca la falta de conocimiento, o compromiso para la aplicación de dichas medidas puede minimizar por medio del uso obligatorio y la mejora continua de las mismas.

Gestión de vulneraciones (plan de acción)

En caso de que la vulneración fuera resultado de la comisión de un delito realizar las denuncias correspondientes.

Llenado de la bitácora de vulneraciones (anexo2) conforme al artículo 39 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y Municipios.

Mecanismos de monitoreo y revisión de las medidas de seguridad (anual)

El monitoreo y evaluación de los sistemas de seguridad se debe realizar para valorar las amenazas, vulnerabilidades, aplicación correcta o incorrecta, impacto y actualización; por lo que se realizarán visitas de manera aleatoria a las áreas (3) con la finalidad de verificar que

se implementa de manera correcta las medidas de seguridad, descritas en el presente documento.

Lo anterior con el objetivo de que las medidas de seguridad continúan siendo efectivas e idóneas.

Plan de trabajo

La existencia del documento de seguridad, busca cumplir con las obligaciones del Instituto respecto a la máxima protección de datos personales. Debido a la importancia y el contexto actual en materia de datos personales, por lo que el presente plan de trabajo, deberá estar en constante actualización, para así alcanzar los objetivos del sistema de seguridad de protección de datos personales.

La finalidad de este plan es crear de manera enunciativa, más no limitativa, las actividades que el Instituto Estatal para la Educación de Jóvenes y Adultos deberá realizar para la aplicación del presente documento de seguridad, en cumplimiento a las facultades establecidas en el la Ley de Protección de Datos Personales en Posesión de sujetos Obligados del Estado de Jalisco y sus Municipios.

Para la ejecución del presente documento de seguridad, dentro de los 12 meses siguientes a la emisión del presente documento: Se emitirá a través de correo institucional la emisión del documento de seguridad, solicitando el apoyo para la difusión interna del mismo, se buscará la participación del Órgano garante y/o de la Coordinación General de Transparencia del Gobierno del Estado de Jalisco para una primera capacitación básica para los servidores públicos que recaban datos personales.

El Comité de Transparencia revisará de manera anual, a partir de la emisión del presente documento de seguridad:
Índice de Datos Personales
Medidas de Seguridad
Plan de trabajo
Capacitaciones internas y/o por organismos competentes en la materia.

Programa General de Capacitación

Se manejarán las capacitaciones de conformidad con las necesidades del Instituto Estatal para la Educación de Jóvenes y Adultos, respecto a la implementación y aplicación del sistema de manejo de datos personales. (Las fechas exactas se les notificarán con al menos una semana de anticipación con la intención de que asista el mayor número posible de interesados)
La capacitación del personal del instituto será de manera cuatrimestral con las siguientes temáticas:

- Generalidades de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados
- Principios y Deberes
- Sistema de Gestión, Medidas de seguridad y acciones preventivas.

Plan de Contingencia para la protección de la información del Instituto Estatal para la Educación de Jóvenes y Adultos (INEEJAD)

Ante la pérdida total o parcial de datos personales en posesión de este sujeto obligado, se debe contar con un plan de contingencia.

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 evolucionan. Por lo que con la aplicación de las medidas de seguridad establecidas en este documento se buscan minimizar los riesgos y/o vulneraciones, pero a su vez se intenta propiciar el restablecimiento de los datos personales en el menor tiempo posible ante cualquier eventualidad. En caso de que los datos personales sufran algún tipo de daño o pérdida, se dispondrá de los respaldos electrónicos realizados por cada área administrativa 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.

Con la evaluación de riesgos y la elaboración de las medidas de seguridad aplicables para prevenir las posibles vulneraciones a las 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 con anterioridad, 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.

Catálogo de Sistemas de Tratamiento de Datos Personales

Sistema de Tratamiento Atención Educativa	
Administrador	Rafael González Jáuregui
Cargo	Analista Administrativo
Área	Dirección de Planeación
Funciones y obligaciones	1. Recibir a los ciudadanos 2. Atender llamadas telefónicas 3. Entregar certificados 4. Tramitar duplicados.
Administrador	Miguel Ángel de la Torre Valdez
Cargo	Operador de información
Área	Departamento de Acreditación
Funciones y obligaciones	1. Validación de datos 2. Elaboración de certificados
Datos Personales que son Recabados	
Inventario de Datos Personales	Nombre Fecha de nacimiento Estado Civil Domicilio Fotografía Edad Sexo Curp Nacionalidad Firma Teléfono Correo Cp. Municipio Estatus laboral Antecedentes escolares
Base de Datos	Sasa, Siga
Controles de Seguridad para la base de datos	Usuario y contraseña personalizada
Estructura y Descripción del Sistema	
Tipo de Soporte	Electrónico
Características del Lugar del Resguardo	Base de datos

Programas en que son Utilizados los Datos Personales	Sistema Sasa y Siga
Resguardo de los Soportes Físicos y/o Electrónicos en que se Encuentran los Datos Personales	
Físicos	No aplica
Electrónicos	Base de datos
Las Bitácoras de Acceso y Operación Cotidiana	
Bitácoras Físicas	Identificación y/o lugar de almacenamiento
Bitácoras Electrónicas	Base de datos
Bitácoras de Vulneración de Seguridad	
Fecha de Vulneración	Hasta el momento ninguna
Motivo de Vulneración	No aplica
Acciones Correctivas	No aplica

Sistema de Tratamiento Control de Seguridad Ingreso	
Administrador	Vigilante de Seguridad
Cargo	Vigilante de Seguridad
Funciones y obligaciones	1. Atención a los ciudadanos, al registro al edificio para alguna realización de algún trámite. 2. Una vez que se concluye la visita, se registra la salida 3. Las demás encomendadas por su superior jerárquico, así como las derivadas de la normatividad aplicable en la materia. 4. Verificar que todo el instituto quede cerrado, cuando todo el personal termino sus labores
Datos Personales que son Recabados	
Inventario de Datos Personales	Nombre Firma
Base de Datos	No aplica
Controles de Seguridad para la base de datos	No aplica
Estructura y Descripción del Sistema	
Tipo de Soporte	Físico
Características del Lugar del Resguardo	Área de vigilancia
Programas en que son Utilizados los Datos Personales	No aplica
Resguardo de los Soportes Físicos y/o Electrónicos en que se Encuentran los Datos Personales	
Físicos	Se encuentran dentro del área de vigilancia
Electrónicos	No aplica
Las Bitácoras de Acceso y Operación Cotidiana	
Bitácoras Físicas	Identificación y/o lugar de almacenamiento
Bitácoras Electrónicas	No aplica

Bitácoras de Vulneración de Seguridad	
Fecha de Vulneración	Hasta el momento ninguna
Motivo de Vulneración	No aplica
Acciones Correctivas	No aplica

Sistema de Tratamiento solicitudes de derecho de acceso a la información.	
Administrador	Martha Alejandra Santiago Toribio
Cargo	Coordinador de Zona
Área	Dirección General
Funciones y obligaciones	1. Recepción y trámite a las solicitudes de derecho de acceso a la información. 2. Las demás encomendadas por su superior jerárquico, así como las derivadas de la normatividad aplicable en la materia.
Datos Personales que son Recabados	
Inventario de Datos Personales	Nombre Domicilio Nacionalidad Correo electrónico Número telefónico
Base de Datos	Electrónica y física
Controles de Seguridad para la base de datos	Usuarios y contraseñas personalizadas
Estructura y Descripción del Sistema	
Tipo de Soporte	Electrónico y físico
Características del Lugar del Resguardo	Se encuentra en una base de datos
Programas en que son Utilizados los Datos Personales	Infomex, Plataforma Nacional de Transparencia, Correo electrónico
Resguardo de los Soportes Físicos y/o Electrónicos en que se Encuentran los Datos Personales	
Físicos	En expedientes dentro de Archiveros
Electrónicos	Base de datos
Las Bitácoras de Acceso y Operación Cotidiana	
Bitácoras Físicas	Identificación y/o lugar de almacenamiento
Bitácoras Electrónicas	Identificación y/o lugar de almacenamiento
Bitácoras de Vulneración de Seguridad	
Fecha de Vulneración	Hasta el momento ninguna
Motivo de Vulneración	No aplica
Acciones Correctivas	No aplica

Sistema de Tratamiento Elaboración de gafete de empleado.	
Administrador	Israel Guizar Lomelí
Cargo	Jefe de Informática
Área	Informática
Funciones y Obligaciones	Gestión general del departamento de informática
Usuario Responsable 1	Leticia Ramírez González Del pliego
Cargo	Programación y código
Área	Informática
Funciones y Cargo	Programación
Usuario Responsable 2	Claudia Isabel Ibarra Martínez
Cargo	Jefe de Oficina
Área	Informática
Funciones y Cargo	Elaboración y entrega de gafete de los empleados
Datos Personales que son Recabados	
Inventario de Datos Personales	Nombre Nombramiento CURP RFC Número del Seguro Social Tipo de sangre Firmas Fotografía Numero de emergencia ID empleado Adscripción
Base de Datos	Electrónica
Controles de Seguridad para la base de datos	Usuarios y contraseñas personalizadas
Estructura y Descripción del Sistema	
Tipo de Soporte	Electrónico
Características del Lugar del Resguardo	Se encuentra en base de datos
Programas en que son Utilizados los Datos Personales	Sistema Institucional de Recursos Humanos
Resguardo de los Soportes Físicos y/o Electrónicos en que se Encuentran los Datos Personales	
Físicos	No aplica
Electrónicos	Se encuentra en base de datos
Las Bitácoras de Acceso y Operación Cotidiana	
Bitácoras Físicas	Identificación y/o lugar de almacenamiento
Bitácoras Electrónicas	Identificación y/o lugar de almacenamiento
Bitácoras de Vulneración de Seguridad	
Fecha de Vulneración	Hasta el momento ninguna
Motivo de Vulneración	No aplica

Acciones Correctivas	No aplica

Sistema de Tratamiento Pago a empleados			
Administrador	Ángel Israel Carrillo Macías	COMPAQ i nominas	6 bases de datos
Cargo:	Director de Área		
Área	Dirección de Tesorería		
Funciones y obligaciones	Efectuar los procesos necesarios para la determinación, supervisión y pago de las diversas obligaciones fiscales a cargo del instituto, que sean determinadas por las diversas legislaciones aplicables. Realizar las transferencias bancarias de pago a terceros por obligaciones patronales. Autorizar, controlar registrar, procesar y distribuir oportunamente el pago quincenal de las nóminas del personal del Instituto. Realizar las transferencias bancarias para el pago de las nóminas quincenales del personal del Instituto.		
Personal autorizado para tratamiento			
Nombre del puesto	Estela Yadira Estupiñan Sandoval	COMPAQ i nominas	6 bases de datos
Funciones y obligaciones:	Elaborar la nómina del personal Institucional y contratado bajo el régimen de honorarios Solicito las incidencias del personal al Departamento de Recursos Humanos y Servicio Social Solicitar el pago a terceros por obligaciones patronales Realizar el envío de los CFDI a los contribuyentes Realizar las retenciones de los impuestos ante Hacienda Solicitar el pago de las retenciones a los empleados por solicitudes de descuento por Condiciones Generales de Trabajo Pago de prestaciones establecidas por contrato colectivo de Trabajo Calculo de retenciones por impuesto ante finiquitos Solicitud de Pago por mandato judicial (descuento por pensión alimenticia) Elaboración de oficios para tramites de seguridad social Certificación de información ante ISSSTE Gestor de movimientos y vigencia ante el ISSSTE (préstamos a corto plazo) Movimientos afiliatorios y vigencia de derechos ante el IMSS Presentación de Calculo anual Revisión y solicitud de expedientes del personal		

	Actualización de información quincenal de la plataforma de Transparencia Estatal como PNT Revisión de Cartera FOVISSSTE y aplicación de préstamos Hipotecarios Elaboración, revisión y entrega de información correspondiente a la Ley General de Contabilidad Gubernamental, Art. 73 Revisión, validación y captura de la plantilla en el sistema de Pensiones del Estado Revisión de base de datos que nos emite el Departamento de Informática para el pago del SAR-FOVISSSTE Revisión de las cifras de control que emite el Departamento de Informática para ser enviada al ISSSTE Recibo y entrego los Vales de despensa anuales al personal autorizado.		
Nombre del puesto	Heriberto Muñiz Guzmán	COMPAQ i nominas	2 bases de datos
Funciones y obligaciones:	Apoyo para elaborar la nómina del personal institucional de base y cuses ramo 33 s Apoyo en la captura de pago de prestaciones establecidas por contrato colectivo de Trabajo Elaboración de archivos comprobatorios para captura de información en los portales de SERICA, SAR-FOVISSSTE y FOVISSSTE		
Tipo de datos personales pertenecientes al sistema de tratamiento de los pagos a empleados			
Inventario:	ID, Nombre, Domicilio, Correo Electrónico, Sexo, Edad, Firma, Fecha De Ingreso, RFC, CURP, Número de Cuenta, Clabe Interbancaria, Teléfono, sueldo mensual, importe neto.		
Bases de datos	COMPAQ i nómina.		
No. De titulares	1900		
Controles de seguridad para las bases de datos	Usuario y Password o Contraseña		
Estructura y descripción del Sistema de tratamiento			
Tipo de soporte:	Físicos y electrónicos		

Características del lugar de resguardo:	Archiveros, Anaqueles, Escritorio, Cajas, así como equipos de cómputo y plataformas
Programas en que se utilizan los D.P.	COMPAQ i nóminas, Excel, Sirh, correo electrónico
Resguardo de los soportes físicos y/o electrónicos en que se encuentran los datos personales	
Físicos	Archiveros, Anaqueles, Escritorio, Cajas, así como equipos de cómputo y plataformas
Electrónicos	Equipo de cómputo con internet que se requiere Usuario y Password o Contraseña. Para su utilización.
Bitácoras de Acceso y Operación Cotidiana	
Bitácoras Físicas	Identificación y/o lugar de almacenamiento
Bitácoras Electrónicas	Identificación y/o lugar de almacenamiento
Bitácoras de Vulneración de Seguridad	
Fecha de Vulneración	Hasta el momento ninguna
Motivo de Vulneración	No aplica
Acciones Correctivas	No aplica

Sistema de Tratamiento Contratación por Honorarios	
Administrador	José Cruz Sánchez Ortega
Cargo	Director de Administración
Área	Dirección de Administración
Funciones y obligaciones	Decreto de Creación 18430 Artículo 20.-El "Instituto" contará con Unidades Técnicas y Administrativas Centrales que tendrán a su cargó la aplicación de la normatividad, evaluación y control de sus actividades, mediante autorización de la Junta de Gobierno y cuyas funciones se establecerán en el Reglamento Interior. Artículo 22.-Las relaciones de trabajo entre el "Instituto" y sus trabajadores se regirán por la Ley para Servidores Públicos y la Ley de Responsabilidades, ambas disposiciones del Estado de Jalisco y las demás disposiciones legales aplicables. Serán considerados trabajadores de confianza: El Director General, Directores y Sub Directores

	de Área, Jefes y Sub Jefes de Departamento, Delegados, Sub Delegados y Coordinadores, el personal de Apoyo Técnico a los Servidores Públicos anteriores y en general todo aquel que realice funciones de dirección, inspección, investigación, supervisión, vigilancia y fiscalización. Artículo 23.-Los trabajadores del Instituto Nacional para la Educación de los Adultos que sean sujetos de transferencia al "Instituto", continuarán incorporados al régimen obligatorio de seguridad social en los términos de la Ley del Instituto de Seguridad y Servicios Sociales de los Trabajadores del Estado, conforme a lo previsto en el convenio de coordinación que para la descentralización de los servicios de educación para los adultos subscribieron con fecha 08 de octubre de 1999, el Ejecutivo Federal por conducto de la Secretaria de Educación Pública, el Ejecutivo del Estado y el Instituto Nacional para la Educación de los Adultos, con la participación de la Federación de Sindicatos de Trabajadores al Servicio del Estado y el Sindicato Único de Trabajadores del Instituto Nacional para la Educación de los Adultos. Los servicios de seguridad social podrán ser prestados por otros organismos cuando así lo convengan el "Instituto" y el Sindicato que agrupa a sus trabajadores de base. Atender las funciones que están plenamente establecidas en los artículos 5 fracción II, 26 Fracción IV, V, VII, IX, XI, XV, XIV, XVI. Art 37, Artículo 30 fracción I, II, III, IV, V, VII, IX, X, XI, XII, XIII, XIV, Art 31 fracción I.
Encargado Responsable 1	Ana Fabiola Lambaren Verdin
Cargo	Jefa del Depto. Recursos Humanos y Servicios Social
Área	Dirección de Administración
Funciones y Obligaciones	Artículo 31 fracción I del Reglamento Interno del IEEA Manual de Percepciones de la Administración Pública Federal Ley del Impuesto sobre la renta Art 30 capítulo III de la Ley de Hacienda del Estado de Jalisco,

	Art 10 de la Ley de Ingresos del Estado de Jalisco Detectar las necesidades en materia de Recursos Humanos y Servicio Social, así como su cumplimiento en su marco normativo
Usuario Responsable 1	Ma Guadalupe Rubio Martin del Campo
Cargo	Técnico Operativo
Área	Dirección Administrativa
Funciones y Obligaciones	Elaboración de los Contratos de Honorarios Asimilables a Salarios Elaboración de Contratos a solicitud y emisión del pago quincenal previo reporte de actividades, así como solicitud de prestador de servicios
Datos Personales que son Recabados	
Inventario de Datos Personales	Nombre Alta del banco Clave interbancaria Cuenta bancaria Domicilio Fotografía Sexo Edad Estatura Peso CURP RFC Correo electrónico Clave Elector
Base de Datos	(SIRH) Sistema Institucional de Recursos Humanos
Controles de Seguridad para la base de datos	Usuarios y Contraseñas
Estructura y Descripción del Sistema	
Tipo de Soporte	Electrónico
Características del Lugar del Resguardo	Se encuentra en una base de datos
Programas en que son Utilizados los Datos Personales	SIRH Sistema Institucional de Recursos Humanos
Resguardo de los Soportes Físicos y/o Electrónicos en que se Encuentran los Datos Personales	
Físicos	Segunda planta oficinas del lado derecho, en archiveros metálicos de 4 gavetas resguardo bajo llave de las oficinas de la Dirección general.

Electrónicos	El Resguardo Electrónico, se localiza en el CPU autorizado por esta Institución el cual lleva el nombre de bitácora de Contratos de Honorarios.
Las Bitácoras de Acceso y Operación Cotidiana	
Bitácoras Físicas	Identificación y/o lugar de almacenamiento
Bitácoras Electrónicas	Identificación y/o lugar de almacenamiento
Bitácoras de Vulneración de Seguridad	
Fecha de Vulneración	Hasta el momento ninguna
Motivo de Vulneración	No aplica
Acciones Correctivas	No aplica

Sistema de Tratamiento servicio social o prácticas profesionales	
Administrador	José Cruz Sánchez Ortega
Cargo	Director de Administración
Área	Dirección de Administración
Funciones y obligaciones	Decreto de Creación 18430 Artículo 20.-El "Instituto" contará con Unidades Técnicas y Administrativas Centrales que tendrán a su cargó la aplicación de la normatividad, evaluación y control de sus actividades, mediante autorización de la Junta de Gobierno y cuyas funciones se establecerán en el Reglamento Interior. Artículo 22.-Las relaciones de trabajo entre el "Instituto" y sus trabajadores se regirán por la Ley para Servidores Públicos y la Ley de Responsabilidades, ambas disposiciones del Estado de Jalisco y las demás disposiciones legales aplicables. Serán considerados trabajadores de confianza: El Director General, Directores y Sub Directores de Área, Jefes y Sub Jefes de Departamento, Delegados, Sub Delegados y Coordinadores, el personal de Apoyo Técnico a los Servidores Públicos anteriores y en general todo aquel que realice funciones de dirección, inspección, investigación, supervisión, vigilancia y fiscalización. Artículo 23.-Los trabajadores del Instituto Nacional para la Educación de los Adultos que

	sean sujetos de transferencia al “Instituto”, continuarán incorporados al régimen obligatorio de seguridad social en los términos de la Ley del Instituto de Seguridad y Servicios Sociales de los Trabajadores del Estado, conforme a lo previsto en el convenio de coordinación que para la descentralización de los servicios de educación para los adultos subscribieron con fecha 08 de octubre de 1999, el Ejecutivo Federal por conducto de la Secretaria de Educación Pública, el Ejecutivo del Estado y el Instituto Nacional para la Educación de los Adultos, con la participación de la Federación de Sindicatos de Trabajadores al Servicio del Estado y el Sindicato Único de Trabajadores del Instituto Nacional para la Educación de los Adultos. Los servicios de seguridad social podrán ser prestados por otros organismos cuando así lo convengan el “Instituto” y el Sindicato que agrupa a sus trabajadores de base. Atender las funciones que están plenamente establecidas en los artículos 5 fracción II, 26 Fracción IV, V, VII, IX, XI, XV, XIV, XVI. Art 37, Artículo 30 fracción I, II, III, IV, V, VII, IX, X, XI, XII, XIII, XIV, Art 31 fracción I.
Encargado Responsable 1	Ana Fabiola Lambaren Verdin
Cargo	Jefa del Depto. Recursos Humanos y Servicios Social
Área	Dirección de Administración
Funciones y Obligaciones	Artículo 31 fracción I del Reglamento Interno del IEEA Manual de Percepciones de la Administración Pública Federal Ley del Impuesto sobre la renta Art 30 capítulo III de la Ley de Hacienda del Estado de Jalisco, Art 10 de la Ley de Ingresos del Estado de Jalisco Detectar las necesidades en materia de Recursos Humanos y Servicio Social, así como su cumplimiento en su marco normativo
Usuario Responsable 1	Ana Beatriz López Briones
Cargo	Técnico Superior
Área	Departamento de Recursos Humanos y Servicio

	Social
Funciones y Obligaciones	Realizar la asignación de prestadores de servicio social, captura de reportes mensuales de actividades, tramite de reporte bimestral, constancia de liberación. Seguimiento a Convenios de Colaboración en materia de Servicio Social. Tramitar solicitud de prestadores de servicio social ante Universidades. Llevar un control de los expedientes de prestadores de servicio social, así como el resguardo de registros electrónicos de cada uno.
Datos Personales que son Recabados	
Inventario de Datos Personales	Nombre Domicilio Teléfono Fotografía Firma Huella digital Nivel de estudios
Base de Datos	Electrónica
Controles de Seguridad para la base de datos	Usuarios y contraseñas personalizadas
Estructura y Descripción del Sistema	
Tipo de Soporte	Físico y Electrónico
Características del Lugar del Resguardo	Los datos se almacenan en archivos electrónicos y físicos con la finalidad de llevar un mejor control, así como la conservación de la información.
Programas en que son Utilizados los Datos Personales	CAPSS (Control Automatizado de Prestadores de Servicio Social)
Resguardo de los Soportes Físicos y/o Electrónicos en que se Encuentran los Datos Personales	
Físicos	Expedientes dentro de archiveros, dentro del Departamento de Servicio Social ubicado en Dirección General y dos archiveros en el edificio de Marsella.
Electrónicos	Usuarios y Contraseñas
Las Bitácoras de Acceso y Operación Cotidiana	
Bitácoras Físicas	Identificación y/o lugar de almacenamiento
Bitácoras Electrónicas	Identificación y/o lugar de almacenamiento
Bitácoras de Vulneración de Seguridad	
Fecha de Vulneración	Hasta el momento ninguna
Motivo de Vulneración	No aplica
Acciones Correctivas	No aplica

Sistema de Tratamiento altas, bajas y modificaciones de nombramientos	
Administrador	José Cruz Sánchez Ortega
Cargo	Director de Administración
Área	Dirección de Administración
Funciones y obligaciones	Decreto de Creación 18430 Artículo 20.-El "Instituto" contará con Unidades Técnicas y Administrativas Centrales que tendrán a su cargó la aplicación de la normatividad, evaluación y control de sus actividades, mediante autorización de la Junta de Gobierno y cuyas funciones se establecerán en el Reglamento Interior. Artículo 22.-Las relaciones de trabajo entre el "Instituto" y sus trabajadores se regirán por la Ley para Servidores Públicos y la Ley de Responsabilidades, ambas disposiciones del Estado de Jalisco y las demás disposiciones legales aplicables. Serán considerados trabajadores de confianza: El Director General, Directores y Sub Directores de Área, Jefes y Sub Jefes de Departamento, Delegados, Sub Delegados y Coordinadores, el personal de Apoyo Técnico a los Servidores Públicos anteriores y en general todo aquel que realice funciones de dirección, inspección, investigación, supervisión, vigilancia y fiscalización. Artículo 23.-Los trabajadores del Instituto Nacional para la Educación de los Adultos que sean sujetos de transferencia al "Instituto", continuarán incorporados al régimen obligatorio de seguridad social en los términos de la Ley del Instituto de Seguridad y Servicios Sociales de los Trabajadores del Estado, conforme a lo previsto en el convenio de coordinación que para la descentralización de los servicios de educación para los adultos subscribieron con fecha 08 de octubre de 1999, el Ejecutivo Federal por conducto de la Secretaria de Educación Pública, el Ejecutivo del Estado y el Instituto Nacional para la Educación de los Adultos, con la participación de la Federación de Sindicatos de Trabajadores al Servicio del Estado y el

	Sindicato Único de Trabajadores del Instituto Nacional para la Educación de los Adultos. Los servicios de seguridad social podrán ser prestados por otros organismos cuando así lo convengan el "Instituto" y el Sindicato que agrupa a sus trabajadores de base. Atender las funciones que están plenamente establecidas en los artículos 5 fracción II, 26 Fracción IV, V, VII, IX, XI, XV, XIV, XVI. Art 37, Artículo 30 fracción I, II, III, IV, V, VII, IX, X, XI, XII, XIII, XIV, Art 31 fracción I.
Encargado Responsable 1	Ana Fabiola Lambaren Verdin
Cargo	Jefa del Depto. Recursos Humanos y Servicios Social
Área	Dirección de Administración
Funciones y Obligaciones	Artículo 31 fracción I del Reglamento Interno del IEEA Manual de Percepciones de la Administración Pública Federal Ley del Impuesto sobre la renta Art 30 capítulo III de la Ley de Hacienda del Estado de Jalisco, Art 10 de la Ley de Ingresos del Estado de Jalisco Detectar las necesidades en materia de Recursos Humanos y Servicio Social, así como su cumplimiento en su marco normativo
Usuario Responsable 1	Leticia Martínez Cárdenas
Cargo	Secretaría
Área	Departamento de Recursos Humanos y Servicio Social
Funciones y Obligaciones	Elaboración de Altas, Bajas, modificaciones, así como la elaboración de nombramientos y generar los expedientes de los empleados y recabar información básica necesaria para la elaboración de los mismos.
Datos Personales que son Recabados	
Inventario de Datos Personales	Nombre Nombramiento CURP RFC Número de Seguridad Social Fecha de Nacimiento Edad

	Tipo de sangre Peso Estatura Alergias Sexo Domicilio Escolaridad Teléfono Estado civil Nacionalidad Correo electrónico Cuenta clave
Base de Datos	Electrónica
Controles de Seguridad para la base de datos	Usuarios y contraseñas personalizadas
Estructura y Descripción del Sistema	
Tipo de Soporte	Físico y Electrónico
Características del Lugar del Resguardo	Los datos se almacenan en archivos electrónicos y físicos con la finalidad de llevar un mejor control, así como la conservación de la información.
Programas en que son Utilizados los Datos Personales	SIRH Sistema Institucional de Recursos Humanos
Resguardo de los Soportes Físicos y/o Electrónicos en que se Encuentran los Datos Personales	
Físicos	Expedientes dentro de archiveros, dentro del Departamento de Recursos Humanos y Servicio Social.
Electrónicos	Usuarios y Contraseñas
Las Bitácoras de Acceso y Operación Cotidiana	
Bitácoras Físicas	Identificación y/o lugar de almacenamiento
Bitácoras Electrónicas	Identificación y/o lugar de almacenamiento
Bitácoras de Vulneración de Seguridad	
Fecha de Vulneración	Hasta el momento ninguna
Motivo de Vulneración	No aplica
Acciones Correctivas	No aplica

Sistema de Tratamiento Adquisiciones, para la realización de las órdenes de compra y servicio.	
Administrador	José Cruz Sánchez Ortega
Cargo	Director de Administración
Área	Dirección de Administración
Funciones y Obligaciones	Las funciones que están plenamente establecidas en el artículo 31 fracción III del reglamento interno del instituto estatal para la educación de los adultos del estado de Jalisco. Así como atender las funciones que están plenamente establecidas en el artículo 30 fracción XXIII, XXIV Y XXV del reglamento interno del Instituto Estatal para la Educación de los Adultos del Estado de Jalisco.
Encargado Responsable 1	Gloria Patricia García Covarrubias
Cargo	Jefe de Departamento encargada de la Unidad Centralizada de Compras
Área	Unidad Centralizada de Compras
Funciones y Obligaciones	Las funciones que están plenamente establecidas en el artículo 31 fracción III del reglamento interno del instituto estatal para la educación de los adultos del estado de Jalisco. Así como atender las funciones que están plenamente establecidas en el artículo 30 fracción XXIII, XXIV Y XXV del reglamento interno del Instituto Estatal para la Educación de los Adultos del Estado de Jalisco.
Usuario Responsable 1	Olimpia Judith Pineda Vidrio
Cargo	Coord de U de Serv Esp en P y P
Área	Unidad Centralizada de Compras
Funciones y Obligaciones	Elaboración de las Bases para las licitaciones, elaboración de actas y el estudio de mercado, tanto técnica como económica. Las demás encomendadas por su superior jerárquico, así como las derivadas de la normatividad.
Usuario Responsable 2	Diego Abraham Pacheco Flores
Cargo	Administrativo Especializado
Área	Unidad Centralizada de Compras
Funciones y obligaciones	Elaborar requisiciones, control de expedientes, control de Pagos mediante órdenes de compras. Las demás encomendadas por su superior jerárquico, así como las derivadas de la normatividad.

Datos Personales que son Recabados	
Inventario de Datos Personales	Registro Único de Proveedores Razón social de persona física RFC Nombre Domicilio Teléfono CURP Fotografía Nacionalidad Firma Huella digital Edad
Base de Datos	Electrónica
Controles de Seguridad para la base de datos	Usuarios y contraseñas personalizadas
Estructura y Descripción del Sistema	
Tipo de Soporte	Electrónico y físico
Características del Lugar del Resguardo	Se encuentra en una base de datos
Programas en que son Utilizados los Datos Personales	No aplica
Resguardo de los Soportes Físicos y/o Electrónicos en que se Encuentran los Datos Personales	
Físicos	En expedientes que se encuentran dentro de los Archiveros
Electrónicos	Base de datos
Las Bitácoras de Acceso y Operación Cotidiana	
Bitácoras Físicas	Identificación y/o lugar de almacenamiento
Bitácoras Electrónicas	Identificación y/o lugar de almacenamiento
Bitácoras de Vulneración de Seguridad	
Fecha de Vulneración	Hasta el momento ninguna
Motivo de Vulneración	No aplica
Acciones Correctivas	No aplica

Sistema de Tratamiento Convenios y Contratos	
Administrador	Lic. Miroslava Genoveva Janet Díaz Hernández
Cargo	Coordinador de Asuntos Jurídicos
Área	Coordinación de Asuntos Jurídicos
Funciones y obligaciones	Atención de todos los Asuntos Jurídicos del Instituto, realización de contratos de Arrendamiento de los inmuebles que ocupan las coordinaciones de zona y demás áreas del Instituto. Elaboración de Convenios de colaboración para el establecimiento y operación de Plazas Comunitarias y Puntos de Encuentro. Elaboración de Contratos de prestación de Servicios de los Proveedores del INEEJAD. Atención de Demandas Laborales.

	Denuncias Penales.
Usuario Responsable 1	Luis David Galván López
Cargo	Jefe de Oficina
Área	Coordinación de Asuntos Jurídicos
Funciones y Obligaciones	Recibir las notificaciones de demandas laborales y demás asuntos relacionados con la coordinación de asuntos Jurídicos.
Usuario Responsable 2	Ernesto Francisco Bernardo Díaz
Cargo	Abogado
Área	Coordinación de Asuntos Jurídicos
Funciones y Obligaciones	Recibir las notificaciones de demandas laborales, elaboración de convenios y demás asuntos relacionados con la coordinación de Asuntos Jurídicos.
Usuario Responsable 3	Aurelio Rivas Navarro
Cargo	Abogado
Área	Coordinación de Asuntos Jurídicos
Funciones y Obligaciones	Recibir las notificaciones de demandas laborales, elaboración de contratos, denuncias penales y demás asuntos relacionados con la coordinación de Asuntos Jurídicos.
Datos Personales que son Recabados	
Inventario de Datos Personales	Nombre Domicilio Fecha de nacimiento Número telefónico RFC CURP Fotografía Estado civil Nacionalidad Huella digital Genero Correo electrónico
Base de Datos	Electrónica
Controles de Seguridad para la base de datos	Usuarios y contraseñas personalizadas
Estructura y Descripción del Sistema	
Tipo de Soporte	Electrónico y física
Características del Lugar del Resguardo	Expedientes se encuentran resguardados en los archiveros y en forma electrónica, los físicos en archivero y el electrónico en archivos de Excel en la pc.
Programas en que son Utilizados los Datos Personales	No aplica
Resguardo de los Soportes Físicos y/o Electrónicos en que se Encuentran los Datos Personales	

Físicos	En expedientes dentro de archiveros
Electrónicos	Se encuentra en una base de datos
Las Bitácoras de Acceso y Operación Cotidiana	
Bitácoras Físicas	Identificación y/o lugar de almacenamiento
Bitácoras Electrónicas	Identificación y/o lugar de almacenamiento
Bitácoras de Vulneración de Seguridad	
Fecha de Vulneración	Hasta el momento ninguna
Motivo de Vulneración	No aplica
Acciones Correctivas	No aplica

Sistema de Tratamiento Investigaciones y Procedimientos Administrativos	
Administrador	Raúl Torres Martínez
Cargo	Contralor
Área	Contraloría Interna
Funciones y obligaciones	1. La integración de las investigaciones y procedimientos administrativos. 2. Las demás encomendadas por su superior jerárquico, así como las derivadas de la normatividad aplicable en la materia.
Datos Personales que son Recabados	
Inventario de Datos Personales	Nombre Teléfono Correo electrónico Dirección
Base de Datos	Electrónica
Controles de Seguridad para la base de datos	Usuarios y contraseñas personalizadas
Estructura y Descripción del Sistema	
Tipo de Soporte	Electrónico y físico
Características del Lugar del Resguardo	Se encuentra en una base de datos
Programas en que son Utilizados los Datos Personales	No aplica
Resguardo de los Soportes Físicos y/o Electrónicos en que se Encuentran los Datos Personales	
Físicos	Expedientes que se encuentran dentro de los archiveros
Electrónicos	Se encuentra en una base de datos
Las Bitácoras de Acceso y Operación Cotidiana	
Bitácoras Físicas	Identificación y/o lugar de almacenamiento
Bitácoras Electrónicas	Identificación y/o lugar de almacenamiento
Bitácoras de Vulneración de Seguridad	
Fecha de Vulneración	Hasta el momento ninguna
Motivo de Vulneración	No aplica
Acciones Correctivas	No aplica

Anexo 1

Bitácora de Acceso	
Nombre y cargo de quien accede	
Identificación del Expediente	
Fojas del Expediente	
Propósito del Acceso	
Fecha de Acceso	
Fecha y hora de Devolución	

Anexo 2

Bitácora de vulneraciones	
Nombre del responsable de la investigación	
Cargo	
Área	
Número de investigación	
Sistema (s) de información o base (s) de dato (s) vulnerado (s)	
Tipo de vulneración	
Tipo de datos personales comprometidos	
Nombre y firma de quien reporta	
Nombre y firma del administrador del sistema	
Nombre y firma del titular del área	