INSTITUTO ESTATAL DE LA EDUCACIÓN PARA LOS ADULTOS DEL ESTADO DE CAMPECHE

CAMPECHE
GOBIERNO DE TODOS

DOCUMENTO DE SEGURIDAD

Instituto Estatal de la Educación para los Adultos
del Estado de Campeche.

Diciembre 2024

GOBIERNO DE TODOS

Contenido

Introducción

El 26 de julio de 2017 se expidió la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Campeche, la cual tiene como objetivo establecer las bases, principios y procedimientos para garantizar el derecho que tiene toda persona a la protección de sus datos personales que estén en posesión de los sujetos obligados.

En su artículo cuarto, La Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Campeche, señala que son sujetos obligados, en el ámbito de validez subjetivo, cualquier autoridad, dependencia, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, Ayuntamientos, órganos, organismos autónomos, tribunales administrativos, fideicomisos y fondos públicos y partidos políticos del orden estatal y municipal del Estado de Campeche que lleven a cabo tratamiento de datos personales.

En ese sentido, el documento de seguridad de los sistemas de datos personales en posesión del Instituto Estatal de la Educación para los Adultos del Estado de Campeche (IEEA) es de observancia obligatoria para todas las personas servidora públicas, y deben observar lo dispuesto por los documentos normativos en el tratamiento de datos personas que lleve a cabo.

De acuerdo con lo dispuesto por los artículos 34 y 35, fracciones I y VII de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Campeche, el responsable deberá implementar mecanismos necesarios para acreditar el cumplimiento de los principios, deberes y obligaciones establecidas en dicha Ley, así como para rendir cuentas al titular y a la comisión, sobre los tratamientos de datos personales que efectúe, para lo cual deberá valerse de los estándares, mejores prácticas nacionales o internaciones o de cualquier otro mecanismo que determine adecuado para tales fines. La Ley dispone que en todo tratamiento de datos personales que realicen los sujetos obligados estará regido por ocho principios y dos deberes. Los ocho principios son: licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad; mientras que los dos deberes son el de confidencialidad y seguridad. Estos principios, deberes y derechos imponen una serie de obligaciones para los sujetos regulados por la Ley, cuya finalidad es que el tratamiento se realice garantizando la protección de los datos personales, con el objeto de respetar el derecho a la autodeterminación informativa de los titulares.

Asimismo, la Ley detalla el alcance y los procedimientos para el ejercicio de los cuatro derechos que el artículo 16 de la Constitución Política de los Estados Unidos Mexicanos reconoce a los titulares de los datos personales: acceso, rectificación, cancelación, y oposición (ARCO), y reconoce uno más, el de portabilidad.

El 15 de febrero de 2018, se publicaron en el Periódico Oficial del Estado de Campeche, los Lineamientos para la Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Campeche, cuyo objetivo es desarrollar las disposiciones previstas en la Ley y, con ello, hacer más comprensible el cumplimiento de los principios, deberes y obligaciones exigidos en materia de protección de datos personales.

En específico, con relación al deber de seguridad, el artículo 50 de la Ley señala que el responsable establecerá las medidas de seguridad técnica y organizativa para garantizar la confidencialidad e integralidad de cada sistema de datos personales que posean con la finalidad de preservar el pleno ejercicio de los derechos tutelados en la Ley, frente a su alteración, pérdida, transmisión y acceso no autorizado, de conformidad con el tipo de datos contenidos en dichos sistemas.

Al Respecto, el artículo 52 de la Ley de Protección de Datos Personales en Posesión de sujetos Obligados del Estado de Campeche señala que para *establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable deberá realizar, al menos, las siguientes actividades interrelacionadas:*

I. Crear políticas internas para la gestión y tratamiento de los datos personales, que tomen en cuenta el contexto en el que ocurren los tratamientos y el ciclo de vida de los datos personales, es decir, su obtención, uso y posterior supresión;

II. Definir las funciones y obligaciones del personal involucrado en el tratamiento de datos personales;

III. Elaborar un inventario de datos personales y de los sistemas de tratamiento;

IV. Realizar un análisis de riesgo de los datos personales, considerando las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento, como pueden ser, de manera enunciativa más no limitativa, hardware, software, personal del responsable, entre otros;

V. Realizar un análisis de brecha, comparando las medidas de seguridad existentes contra las faltantes en la organización del responsable;

VI. Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, así como las medidas para el cumplimiento cotidiano de las políticas de gestión y tratamiento de los datos personales;

VII. Monitorear y revisar de manera periódica las medidas de seguridad implementadas, así como las amenazas y vulneraciones a las que están sujetos los datos personales, y

VIII. Diseñar y aplicar diferentes niveles de capacitación del personal bajo su mando, dependiendo de sus roles y responsabilidades respecto del tratamiento de los datos personales.

Por su parte, el artículo 55 de la Ley de Protección de Datos Personales en Posesión de sujetos Obligados del Estado de Campeche establece como una obligación la elaboración y aprobación de un documento que contenga las medidas de seguridad de carácter físico, técnico y administrativo adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee.

Glosario.

ARCO: Acceso, rectificación, cancelación y oposición.

Datos Personales: cualquier información concerniente a una persona física identificada o identificable expresada en forma numérica, alfabética, alfanumérica, grafica, fotográfica, acústica o en cualquier otro formato. Se considera que una persona es identificable cuando su identidad puede determinarse directa o indirectamente a través de cualquier información, siempre y cuando este no requiera plazas, medios o actividades desproporcionadas.

Derechos ARCO: Los derechos de acceso, rectificación y cancelación de datos personales, así como la oposición al tratamiento de los mismos.

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.

Educación para Personas Adultas.- Considerada una educación a lo largo de la vida y está destinada a la población de quince años o más que no haya cursado o concluido su educación primaria y secundaria. Se presta a través de servicios de alfabetización, educación primaria y secundaria, así como de formación para el trabajo, con las particularidades adecuadas a dicha población.

Figuras operativas. - Son las figuras institucionales, figuras solidarias o personas voluntarias beneficiarias de un subsidio que apoyan la operación de los servicios educativos que ofrecen el INEA o los IEEA;

INEA.- Instituto Nacional para la Educación de los Adultos. Organismo público descentralizado de la APF, agrupado en el sector coordinado por la SEP, con personalidad jurídica y patrimonio propio, con domicilio en la Ciudad de México, que tiene por objeto promover y realizar acciones para organizar e impartir la educación para las personas adultas, a través de la prestación de los servicios de alfabetización, educación primaria, secundaria, la formación para el trabajo y los demás que determinen las disposiciones jurídicas y los programas aplicables apoyándose en la participación y solidaridad social.

IEEA.- Instituto Estatal de la Educación para los Adultos del Estado de Campeche.

LPDPPSOEC: Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Campeche;

LTAIPEC: Ley de Transparencia y Acceso a la Información Pública del Estado de Campeche;

PVBS: Persona voluntaria beneficiaria del subsidio. - Es aquella persona que de forma individual y voluntaria coadyuva en la atención educativa que ofrecen los IEEA, INEA y Plazas Comunitarias en el Exterior y que su participación puede ser susceptible a recibir un apoyo económico.

SCOF.- Sistema de Control de Figuras Operativas: Sistema Informático donde se registran los apoyos económicos otorgados a las figuras operativas.

Sistema de tratamiento y/o Base de datos personales: conjunto ordenado de datos personales referentes a una persona física identificada o identificable, condicionado a criterios determinados que permitan su tratamiento, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización;

Soporte electrónico: Son los medios de almacenamiento, entendible sólo mediante el uso de algún aparato con circuitos electrónicos que procese su contenido para examinar, modificar o almacenar los datos; es decir, cintas magnéticas de audio, vídeo y datos, fichas de microfilm, discos ópticos (CDs y DVDs), discos magneto-ópticos, discos magnéticos (flexibles y duros) y demás medios de almacenamiento masivo no volátil;

Soporte físico: Son los medios de almacenamiento legibles a simple vista, como por ejemplo, documentos, oficios, formularios impresos llenados “a mano” o “a máquina”, fotografías, placas radiológicas, carpetas, expedientes, entre otros;

Tratamiento: cualquier operación o conjunto de operaciones efectuadas mediante procedimientos físicos o automatizados aplicados a los datos personales, relacionadas, de manera enunciativa más no limitativa, con la obtención, uso, registro, organización, conservación, elaboración, utilización, estructuración, adaptación, modificación, extracción, consulta, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, transferencia y, en general, cualquier uso o disposición de datos personales.

Unidad de Transparencia: Según la fracción XXII del artículo 3 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Campeche, es el área responsable, en cada sujeto obligado, de atender y dar trámite a las solicitudes de acceso a la información.

I. Nombre de los sistemas de tratamiento o base de datos personales.

Nombre de la unidad administrativa	Unidad de Informática, Departamento de Acreditación
Fecha de elaboración	17 de octubre del 2024
Fecha de última actualización	17 de octubre del 2024
Nombre del tratamiento	Certificados Enviados. (Pre-registro en Línea para PVBS)
Fundamento jurídico que habilita el tratamiento	Ley de Transparencia y Acceso a la Información Pública del Estado de Campeche Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Campeche Reglamento Interior del IEEA, etc. o alguna otra normatividad aplicable.
Atribuciones de la unidad administrativa para realizar el tratamiento	Creación del formulario de **Pre-registro en Línea para PVBS** y publicación en la página web de la institución.

Nombre de la unidad administrativa	Área de Recursos Humanos
Fecha de elaboración	17 de octubre del 2024
Fecha de última actualización	17 de octubre del 2024
Nombre del tratamiento	Archivero
Fundamento jurídico que habilita el tratamiento	Ley de Transparencia y Acceso a la Información Pública del Estado de Campeche Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Campeche Reglamento Interior del IEEA
Atribuciones de la unidad administrativa para realizar el tratamiento	Responsable de la elaboración de las nóminas ordinarias y extraordinarias

Nombre de la unidad administrativa	Departamento de Planeación y Seguimiento Operativo
Fecha de elaboración	18 de octubre de 2024
Fecha de última actualización	24 de octubre de 2024
Nombre del tratamiento	Sistema de Control de Figuras Operativas
Fundamento jurídico que habilita el tratamiento	Artículos 58 y 67 de la Ley General de Contabilidad Gubernamental
Atribuciones de la unidad administrativa para realizar el tratamiento	Contar con los instrumentos necesarios que nos permitan disponer de la información programática presupuestal, correspondiente a los recursos que son autorizados bajo el marco que establece el Presupuesto de Egresos de la Federación

Nombre de la unidad administrativa	Departamento de Administración
Fecha de elaboración	21/10/2024
Fecha de última actualización	21/10/2024
Nombre del tratamiento	Solicitud de ejercicio de derechos ARCO.
Fundamento jurídico que habilita el tratamiento	Artículo 51 fracción II de la LTAIPEC.
Atribuciones de la unidad administrativa para realizar el tratamiento	Recibir y dar trámite a las solicitudes de acceso a la información

Nombre de la unidad administrativa	Departamento de Administración
Fecha de elaboración	21/10/2024
Fecha de última actualización	21/10/2024
Nombre del tratamiento	Solicitud de acceso a la información
Fundamento jurídico que habilita el tratamiento	Artículo 51 fracción II de la LTAIPEC.
Atribuciones de la unidad administrativa para realizar el tratamiento	Recibir y dar trámite a las solicitudes de acceso a la información

II. El nombre, cargo y adscripción del administrador de cada sistema de tratamiento yo base de datos personales

Nombre del sistema de tratamiento y/o base de datos personales	Cargo y adscripción del administrador
Certificados Enviados. (Pre-registro en Línea para PVBS)	Ing. José Carlos Ramírez Uc. Responsable del Área de Mantenimiento y Desarrollo de Sistemas. Unidad de informática.
	Mtra. Laura Angelica May Salazar Jefa del Departamento de Acreditación Departamento de Acreditación
Expedientes.	L.C. Yunuelly Guadalupe Moreno Vargas. Jefa del Área de Recursos Humanos. Área de Recursos Humanos.
Sistema de Control de Figuras Operativas	C.P. Josefina Jiménez Martínez. Jefa de Departamento. Departamento de Planeación y Seguimiento Operativo.
	Lic. Ana Nallely Flores Denegri. Responsable del Área de Programación y Presupuesto. Departamento de Planeación y Seguimiento Operativo.
Solicitud de ejercicio de derechos ARCO.	C.P. José Antonio Chablé Polanco. Jefe de Departamento de Administración. Departamento de Administración.
Solicitud de acceso a la información	C.P. José Antonio Chablé Polanco. Jefe de Departamento de Administración. Departamento de Administración.

III. Las funciones y obligaciones del responsable, encargados y todas las personas que traten datos personales.

Sistema de tratamiento y/o base de datos personales	Funciones y obligaciones
Certificados Enviados.	Mantener en correcto funcionamiento del formulario de la página web.
	Actualizar la base de datos de información.
	Recopilar la información de certificados enviados en un archivo digital.
	Enviar información para la actualización en el servidor del IEEA.
	Enviar usuarios y contraseñas a cada Delegado Municipal por oficio.
	Mantener actualizada la información de manera mensual.
Expedientes.	Controlar y supervisar la elaboración de los expedientes que contienen todos los datos personales y el resguardo y buen uso de la información contenida.
Sistema de Control de Figuras Operativas.	Administrador: Es el usuario que controla y ejecuta todas las actividades de Sistema de Control de Figuras Operativas y asignar usuarios.
	Capturista: Es el encargado de asignar los datos correspondientes al pago otorgado (número de oficio, fuente de financiamiento, proyecto, fecha). También es responsable de procesar los pagos de productividad y pago fijo (subidos al sistema en formato de Excel), descargar reportes de acuerdo a la información que se requiera.
Solicitud de ejercicio de derechos ARCO.	Dar atención a las solicitudes de ejercicio de derechos ARCO que se presenten ante el Instituto, como responsable del tratamiento de los datos personales.
Solicitud de acceso a la información.	Recibir y dar trámite a las solicitudes de acceso a la información que se presenten ante el Instituto, como responsable del tratamiento de los datos personales.

IV. Inventario de datos personales tratados en cada sistema de tratamiento y/o base de datos personales.

Nombre del sistema de tratamiento o bases de datos personales	Categorías de datos personales	Datos personales	Fundamento legal
Certificados Enviados.	Datos de identidad.	• Nombre. • Clave Única de Registro de Población (CURP).	Artículo 32 fracciones I y II del Reglamento Interior del IEEA.
	Datos electrónicos.	• Correo electrónico.	
	Datos académicos.	• Último grado de estudios.	
	Datos afectivos y/o familiares.	• Estado Civil.	
Expedientes.	Datos de identidad.	• Nombre. • Registro Federal de Contribuyentes (RFC). • Clave Única de Registro de Población (CURP). • Domicilio particular. • Teléfono particular. • Lugar y fecha de nacimiento. • Edad. • Fotografía.	Artículo 30 fracción I del Reglamento Interior del IEEA.
	Datos electrónicos.	• Correo electrónico no oficial.	
	Datos laborales.	• Datos sobre su nombramiento. • Incidencias. • Capacitación. • Desarrollo profesional.	
	Datos patrimoniales.	• Cuenta bancaria. • Seguro de vida institucional y de gastos médicos.	
	Datos académicos.	• Último grado de estudios. • Título. • Cédula profesional.	
	Datos sobre salud.	• El expediente clínico de cualquier atención médica. • Incapacidades médicas.	
	Datos afectivos y/o familiares.	• Estado civil. • Dependientes económicos. • Número de hijos.	

Nombre del sistema de tratamiento o bases de datos personales	Categorías de datos personales	Datos personales	Fundamento legal
Sistema de Control de Figuras Operativas.	Datos de Identidad.	• Nombre de beneficiarios de programas sociales. • Registro Federal de Contribuyentes (RFC). • Clave Única de Registro de Población (CURP). • Domicilio Particular.	Artículo 24 fracciones II y III del Reglamento Interior del IEEA.
	Datos personales de naturaleza pública.	• Percepciones de recursos públicos.	Artículos 58 y 67 de la Ley General de Contabilidad Gubernamental. Ley de Transparencia y Acceso a la Información Pública del Estado de Campeche.
Solicitud de ejercicio de derechos ARCO.	Datos de identidad.	• Nombre del titular o representante. • Domicilio. • Identificación oficial.	Artículos 73, 76, 78, 82 y 117 de la LPDPPSOEC.
	Datos electrónicos.	• Correo electrónico personal.	
Solicitud de acceso a la información.	Datos de identidad.	• Nombre completo. • Domicilio.	Artículo 51 fracción II de la LTAIPEC.
	Datos electrónicos.	• Correo electrónico.	

La obtención de los datos es de manera personal o directa de los titulares, quien presenta la documentación necesaria para cumplir con los trámites solicitados.

V. Estructura y descripción de los sistemas de tratamiento y/o bases de datos personales señalando el tipo de soporte y las características del lugar donde se resguardan.

Nombre del sistema de tratamiento o bases de datos personales	Tipo de Soporte	Características del lugar de resguardo	Programas en los que se utilizan (acceso, manejo, aprovechamiento, procesamiento) los Datos Personales
Certificados Enviados. (Pre-registro en Línea para PVBS).	Electrónico: Páginas web.	Electrónico: Servidor Institucional. Procesador inter xeron e3-1225v5 3.30ghz. Ram: 32gb, con acceso restringido con clave y contraseña. Sistema: Windows server 2012 r2 standar Almacenamiento: 1Tb.	My Sql. Paquetería Office: Excel
Expedientes.	Físico: Documentos.	Físico: Archiveros en el área de Recursos Humanos, bajo llave; en el edificio de la dirección general del IEEA. en Calle Prolongación Allende S/N, entre Av. Luis Donaldo Colosio y calle Privada, Colonia San Rafael, C.P. 24090; San Francisco de Campeche, Campeche.	Paquetería Office.
Sistema de Control de Figuras Operativas	Electrónico: Base de datos.	Electrónico: Servidor Institucional Procesador inter xeron e3-1225v5 3.30ghz Ram: 32gb, con acceso restringido con clave y contraseña. Sistema: Windows server 2012 r2 standar Almacenamiento: 1Tb	Paquetería Office: Microsoft Excel Formato de Documento Portátil (PDF)
Solicitud de ejercicio de derechos ARCO.	Físico: Documentos y expedientes	Físico: Calle Prolongación Allende S/N, entre Avenida Luis Donaldo Colosio y Calle Privada, Colonia San Rafael, C.P. 24090, planta alta. Unidad de Transparencia, esta información se encuentra en los cajones del archivero metálico de 3 cajones, bajo llave.	Paquetería office: Word, Excel Formato de Documento Portátil (PDF)

	Electrónico: Expedientes electrónicos, SISAI	Electrónico: computadora de escritorio marca HP modelo7540, con acceso restringido con clave y contraseña. http://www.plataformadetrasparencia.campeche.org.mx	
Solicitud de acceso a la información.	Físico: Documentos y expedientes	Físico: Calle Prolongación Allende S/N, entre Avenida Luis Donaldo Colosio y Calle Privada, Colonia San Rafael, C.P. 24090, planta alta. Unidad de Transparencia, esta información se encuentra en los cajones del archivero metálico de 3 cajones, bajo llave.	Paquetería office: Word, Excel Formato de Documento Portátil (PDF)
	Electrónico: Expedientes electrónicos, SISAI	Electrónico: computadora de escritorio marca HP modelo7540, con acceso restringido con clave y contraseña. http://www.plataformadetrasparencia.campeche.org.mx	

VI. Controles y mecanismos de seguridad para las transferencias que se efectúen.

Certificados Enviados.	
Transmisiones mediante el traslado físico de soportes electrónicos	La información en archivo de Excel es enviada por el correo electrónico institucional cuya clave de usuario y contraseña está en poder de la Jefa del Departamento de Acreditación y es la única persona que lo utiliza.
Transmisiones mediante el traslado sobre redes electrónicas	El envío de información se lleva a cabo por medio de correo institucional oficial. El archivo de Excel se traslada de la cuenta de correo de la Jefa del Departamento de Acreditación a la cuenta de correo de la Jefa de la Unidad de Informática, usando el servicio de correo electrónico de la red institucional.

Expedientes	
Transmisiones mediante el traslado de soportes físicos	No aplica. Los expedientes no deben abandonar ni el área de resguardo, ni el Instituto a menos que sea previamente autorizado para trasladar el archivo a la bodega de almacenamiento

Sistema de Control de Figuras Operativas	
Transmisiones mediante el traslado físico de soportes electrónicos	Se entrega por medio un oficio y anexo el disco compacto con sesión cerrada para evitar la manipulación de la información guarda, el cual firma de recibido
Transmisiones mediante el traslado sobre redes electrónicas	Envío de información por medio de correo institucional oficial.

Solicitud de ejercicio de derechos ARCO.	
Transmisiones mediante el traslado de soportes físicos	El envío se realiza a través del personal adscrito a los informes generados en la institución, mediante autorización de su superior jerárquico y con oficio de comisión y/o permiso. 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. Toda entrega de información requiere acuse de recibido. A partir de la aprobación del presente documento todas las transmisiones serán registradas en las bitácoras de transferencia de cada área.
Transmisiones mediante el traslado físico de soportes electrónicos	El envío se realiza a través del personal adscrito a los informes generados en la institución, mediante autorización de su superior jerárquico y con oficio de comisión y/o permiso. 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. Toda entrega de información requiere acuse de recibido. A partir de la aprobación del presente documento todas las transmisiones serán registradas en las bitácoras de transferencia de cada área. A partir de la aprobación del presente documento todos los soportes electrónicos que sean transferidos y contengan información confidencial deberán estar protegidos con formatos codificados.
Transmisiones mediante el traslado sobre redes electrónicas	El envío se realiza a través del personal adscrito a los informes generados en la institución, mediante autorización de su superior jerárquico y únicamente a través de medios electrónicos institucionales.

Solicitud de acceso a la información	
Transmisiones mediante el traslado de soportes físicos	El envío se realiza a través del personal adscrito a los informes generados en la institución, mediante autorización de su superior jerárquico y con oficio de comisión y/o permiso. 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. Toda entrega de información requiere acuse de recibido. A partir de la aprobación del presente documento todas las transmisiones serán registradas en las bitácoras de transferencia de cada área.
Transmisiones mediante el traslado físico de soportes electrónicos	El envío se realiza a través del personal adscrito a los informes generados en la institución, mediante autorización de su superior jerárquico y con oficio de comisión y/o permiso. 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. Toda entrega de información requiere acuse de recibido. A partir de la aprobación del presente documento todas las transmisiones serán registradas en las bitácoras de transferencia de cada área. A partir de la aprobación del presente documento todos los soportes electrónicos que sean transferidos y contengan información confidencial deberán estar protegidos con formatos codificados.
Transmisiones mediante el traslado sobre redes electrónicas	El envío se realiza a través del personal adscrito a los informes generados en la institución, mediante autorización de su superior jerárquico y únicamente a través de medios electrónicos institucionales.

VII. Resguardo de los soportes físicos y/o electrónicos de los datos personales del sistema.

a) Resguardo físico

Nombre del sistema de tratamiento o bases de datos personales			Expedientes.			
EQUIPO	**BAJO RESGUARDO**	**CARGO**	**MARCA**	**MODELO**	**SERIE**	**PLAZO DE RESGUARDO**
Departamento de Administración (Área de Recursos Humanos)						
Archivero.	L.C. Yunuelly Guadalupe Moreno Vargas.	Jefa del Área de Recursos Humanos.	N/A.	N/A.	I450400016002602	N/A
Archivero.	L.C. Yunuelly Guadalupe Moreno Vargas.	Jefa del Área de Recursos Humanos.	N/A.	N/A.	I4504000160019202	N/A
Archivero.	L.C. Yunuelly Guadalupe Moreno Vargas.	Jefa del Área de Recursos Humanos.	N/A.	N/A.	I4504000160019602	N/A
Archivero.	L.C. Yunuelly Guadalupe Moreno Vargas.	Jefa del Área de Recursos Humanos.	N/A.	N/A.	NC-016-ALM-00001-20	N/A

Nombre del sistema de tratamiento o bases de datos personales			Solicitud de ejercicio de derechos ARCO.			
EQUIPO	**BAJO RESGUARDO**	**CARGO**	**MARCA**	**MODELO**	**SERIE**	**PLAZO DE RESGUARDO**
Administración.						
Archivero 3 cajones	José Antonio Chablé Polanco	Jefe de Departamento de Administración	s/n	s/n	I-450400016-00002-22	6 años

Nombre del sistema de tratamiento o bases de datos personales			Solicitud de acceso a la información.			
EQUIPO	**BAJO RESGUARDO**	**CARGO**	**MARCA**	**MODELO**	**SERIE**	**PLAZO DE RESGUARDO**
Administración.						
Archivero 3 cajones	José Antonio Chablé Polanco	Jefe de Departamento de Administración	s/n	s/n	I-450400016-00002-22	6 años

b) Resguardo electrónico

Nombre del sistema de tratamiento o bases de datos personales	**Certificados Enviados**				
EQUIPO	**BAJO RESGUARDO**	**CARGO**	**MARCA**	**MODELO**	**SERIE**
Unidad de Informática y Departamento de Acreditación.					
SERVIDORWEB	Ing. Cynthia Amabilis Vivas	Jefa de la unidad de informática	Lenovo	Thinkserver Ts150	mj04ndtx
Computadora portátil Laptop	Laura Angelica May Salazar	Jefa del Departamento de Acreditación	LENOVO	S/N	S/N
Nombre del sistema de tratamiento o bases de datos personales	**Sistema de Control de Figuras Operativas**				
EQUIPO	**BAJO RESGUARDO**	**CARGO**	**MARCA**	**MODELO**	**SERIE**
Unidad de Informática.					
SERVIDORWEB	Ing. Cynthia Amábilis Vivas	Jefa de la unidad de informática	Lenovo	Thinkserver Ts150	mj04ndtx

Nombre del sistema de tratamiento o bases de datos personales	**Solicitud de ejercicio de derechos ARCO.**				
EQUIPO	**BAJO RESGUARDO**	**CARGO**	**MARCA**	**MODELO**	**SERIE**
Administración.					
computadora de escritorio	José Antonio Chablé Polanco	Jefe de Departamento de Administración	marca HP	modelo7540	CNN63107W4
Nombre del sistema de tratamiento o bases de datos personales	**Solicitud de acceso a la información.**				
EQUIPO	**BAJO RESGUARDO**	**CARGO**	**MARCA**	**MODELO**	**SERIE**
Administración.					
computadora de escritorio	José Antonio Chablé Polanco	Jefe de Departamento de Administración	marca HP	modelo7540	CNN63107W4

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

Se utilizan bitácoras de acceso en soportes físicos únicamente en los casos en que personal ajeno a los responsables de los sistemas de tratamiento o base de datos personales requieran acceder a la información contenida en ellos, o bien, en los casos en los cuales tratándose de soportes físicos estos se encuentren en el archivo de concentración por haber fenecido su periodo de trámite, para lo cual se requerirá, además de la autorización del responsable del sistema de tratamiento o base de datos personales, la autorización del responsable del archivo de concentración, conforme a los procedimientos archivísticos establecidos. Para los casos en que se requiera extraer algún equipo de cómputo o cualquier otro activo electrónico que contenga datos personales se deberá solicitar la autorización correspondiente mediante el llenado del ANEXO 1.

Para que los soportes puedan salir de las instalaciones u oficinas, el responsable debe autorizarlo, adoptando para su traslado medidas que eviten la sustracción, pérdida o acceso indebido a la información, indicando las medidas y procedimientos previstos. Siempre que en dado caso, se proceda al traslado de soportes físicos, así como de soportes electrónicos (CORREOS ELECTRÓNICOS) que contengan datos personales, deberá adoptarse las siguientes medidas: El responsable del sistema debe autorizar el traslado del expediente; el mensajero o la persona que traslada el expediente debe ser una persona servidora pública del IEEA, el cual se compromete a adoptar las medidas de seguridad y el deber de secrecía en el manejo de los expedientes; los expedientes deben de ir en sobre debidamente cerrado; los expedientes deben de contener la siguiente leyenda de seguridad. “se hace de su conocimiento que esta información es considerada como confidencial porque contiene los datos personales ANEXO 2”

Las bitácoras de acceso a los datos personales (ANEXO 3) en soportes físicos contienen lo siguiente:

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

Se consideran como “incidencias de seguridad” entre otras, cualquier incumplimiento de la normativa desarrollada en el documento de seguridad, así como cualquier anomalía que afecte o pueda afectar la seguridad de los datos de carácter personal en el sistema. De igual manera la persona que se percate de la incidencia, emitirá un reporte de los hechos mediante este formato, las incidencias deberán ser documentadas para delimitar responsabilidades mediante este Anexo 4 “VULNERACIONES A LA SEGURIDAD DE DATOS PERSONALES” la cual contienen lo siguiente:

- Fecha del incidente.
- Nombre y cargo.
- Área de adscripción.
- Responsable del área.
- Sistema de tratamiento o base de datos personales vulnerada.
- Cantidad de titulares vulnerados.
- Soporte de la información vulnerada.
- Tipo de vulneración.
- Tipo de dato personal afectado.
- Nombre y firma de quien reporta.
- Nombre y firma del administrador del sistema.

IX. Análisis de Riesgos.

El artículo 56, fracción IX de la Ley de Protección de Datos Personales en Posesión de sujetos Obligados establece como una de las actividades a realizar para implementar y mantener medidas de seguridad para la protección de datos personales, la realización del análisis de riesgos, considerando las amenazas y vulneraciones existentes para los datos personales y los recursos involucrados en su tratamiento, como pueden ser de manera enunciativa mas no limitativa, hardware, software, personal del responsable, entre otros.

Análisis de riesgos de infraestructura tecnológica y recursos de software y hardware.

Se realiza de manera general y en específico en los sistemas o base de datos de Certificados Enviados Control de figuras operativas, en los que se lleva a cabo diversos tratamientos que realiza el IEEA, por lo que los riesgos y controles que se determinen aplican directamente a estos.

Activo: Información de la base de datos, esta información viaja por medios electrónicos institucionales. El valor del activo es equivalente a un día de trabajo del Jefe de Departamento.

Amenaza: La amenaza es que algún usuario accese a la computadora lap top y robe los archivos.

Vulnerabilidades: La computadora está conectada a la red institucional.

Medidas preventivas para controlar el riesgo:

1. La información en archivo de Excel es enviada por el correo electrónico institucional cuya clave de usuario y contraseña está en poder de la Jefa del Departamento de Acreditación y es la única persona que lo utiliza.
2. El archivo de Excel se traslada de la cuenta de correo de la Jefa del Departamento de Acreditación a la cuenta de correo de la Jefa de la Unidad de Informática, usando el servicio de correo electrónico de la red institucional.
3. Si se robaran la información se cuenta con un respaldo en el correo electrónico de la Jefa del Departamento de Acreditación y de Informática.
4. Organizar y controlar el resguardo, almacenamiento y manejo de la información en los equipos de cómputo.

Activo	Valor Activo por dimensión			Impacto	Probabilidad	Amenazas
	C	I	D			
Certificados enviados	1	1	1	1 = muy bajo.	4- alta Justificación: el entorno es susceptible a cambios climatológicos impredecibles.	Fenómeno climático (ambiental).
	1	2	3	2= bajo.	3- media Justificación el entorno tiene problemas con el suministro de energía eléctrica.	Pérdida de suministro de energía eléctrica.

	3	3	2	3 = media.	2- baja Justificación: se tiene registro de un intento de espionaje en los últimos 4 años.	Espionaje remoto. (deliberada).
	1	2	1	1 = muy bajo.	1 muy baja Justificación: no se tiene registro de falla de software principal.	Mal funcionamiento del software (deliberada, accidental).
	1	1	3	2= bajo.	2- baja Justificación se tiene registro de un daño al servidor hace más de 5 años.	Mal funcionamiento del equipo (deliberada, accidental).
	3	3	3	3= media.	1 muy baja Justificación no se tiene registro de corrupción de datos.	Corrupción de datos (deliberada, accidental).
	4	4	4	4 = alta.	2- baja Justificación se tiene el registro de un acceso no autorizado hace más de 7 años.	Uso no autorizado de equipos. (deliberada).

Activo	Valor Activo por dimensión			Impacto	Probabilidad	Amenazas
	C	I	D			
Sistema de Control de Figuras Operativas	1	1	1	1 = muy bajo.	4- alta Justificación: el entorno es susceptible a cambios climatológicos impredecibles.	Fenómeno climático (ambiental).
	1	2	1	1 = muy bajo.	1 muy baja Justificación: no se tiene registro de falla de software principal.	Mal funcionamiento del software (deliberada, accidental).
	1	1	3	2= bajo.	2- baja Justificación se tiene registro de un daño al servidor hace más de 5 años.	Mal funcionamiento del equipo (deliberada, accidental).

Análisis de riesgos de hábitos de las personas servidoras públicas del IEEA.

En este, se refiere a los hábitos de seguridad de las personas servidoras públicas de manera general y no asociado a un tratamiento en lo particular.

Medidas preventivas para controlar el riesgo:

1. Garantizar el deber de secrecía en el tratamiento de los datos personales, para las mejores prácticas en el lugar de trabajo.
2. Proponer mecanismos para asegurar que los datos personales en posesión de la unidad administrativa en el ejercicio de sus facultades, no se difundan, distribuyan o comercialicen.
3. Garantizar la seguridad y confidencialidad de los datos personales y evitar su alteración, pérdida, transmisión y acceso no autorizado.
4. Conocer y observar las medidas, normas, procedimientos, reglas y estándares que afecten a las funciones que desarrolla.
5. Notificar las incidencias de seguridad de las que tengan conocimiento respecto a los recursos protegidos, según los procedimientos establecidos en este documento, en concreto en el ANEXO 4.

X. Análisis de Brecha.

En este apartado se consideran las medidas existentes y efectivas; las medidas de seguridad faltantes y la existencia de nuevas medidas de seguridad que pudieran remplazar a uno o más controles implementados en los activos.

Activo	Amenaza	Valor Activo por dimensión			Impacto	Probabilidad	Medidas de seguridad que operan correctamente
		C	I	D			
Certificados enviados	Fenómeno climático.	1	1	1	1 = muy bajo	4- alta Justificación: el entorno es susceptible a cambios climatológicos impredecibles	Reporte del mantenimiento del Proveedor.
	Mal funcionamiento del software.	1	2	1	1 = muy bajo	1 muy baja Justificación: no se tiene registro de falla de software principal	Reporte de mantenimiento de equipo del site.
	Mal funcionamiento del equipo.	1	1	3	2= bajo	2- baja Justificación se tiene registro de un daño al servidor hace más de 5 años	Reporte de mantenimiento de equipo del site.

XI. Gestión de vulneraciones.

Plan de respuesta a las vulneraciones de Seguridad de la Información.

- Realizar mantenimiento preventivo a las instalaciones para evitar filtraciones.
- Realizar mantenimiento preventivo y /o correctivo a el software para su buen funcionamiento.
- Realizar mantenimiento preventivo y /o correctivo a el hardware para su buen funcionamiento.
- Restauración inmediata de la operatividad mediante los respaldos de los soportes electrónicos y versiones digitales de los soportes físicos.
- Las personas que manejan los sistemas electrónicos de protección de datos personales accederán a estos mediante de nombres de usuarios personalizados y contraseñas cifradas para su protección, las cuales permiten el acceso a determinadas funciones del sistema en particular y no en general, dependiendo de su función.
- En caso de que la vulneración fuera resultado de la comisión de un delito realizar las denuncias correspondientes.
- Llenado del formato de vulneraciones a la seguridad de datos personales por parte de la persona que detectó la vulneración.
- Determinación de la magnitud de la afectación y elaboración de recomendaciones para los titulares.
- Elaboración de Informe y propuesta de medidas correctivas a corto y mediano plazo por parte de la Unidad de Transparencia.
- Notificación a titulares en un lapso de 72 horas que de forma significativa vea afectados sus derechos patrimoniales o morales.
- De igual manera, para desechar cualquier soporte que contenga datos de carácter personal deberá destruirse o borrarse, adoptando medidas dirigidas a evitar el acceso a la información contenida en el mismo o su recuperación posterior, levantando la constancia respectiva de su destrucción o eliminación.

XII. Medidas de seguridad implementadas.

A. Medidas de seguridad físicas

Para garantizar la seguridad física de las instalaciones, personas y equipos de la institución se cuenta con procedimientos de control y prevención ante amenazas al entorno físico dentro de los diferentes sistemas de datos personales ya sea de los datos o de los recursos involucrados en su tratamiento, los cuales se describen a continuación, en cada sistema de datos personales y/o base de datos:

Certificados Enviados			
Medidas de seguridad físicas	**Medida**	**Finalidad**	**Descripción**
	Prevenir el acceso no autorizado físico a al site del servidor.	Limitar el acceso a personal no autorizado.	El área donde se encuentra los datos está cerrada bajo llave restringiendo el acceso.
	Bitácora registro de acceso al site.	Tener registro de los datos de la persona que accede a site y el motivo del acceso.	La persona que tiene acceso se registra en una bitácora y anota el motivo por el que accede.
	Mantenimiento preventivo trimestral al servidor.	Mantener en Correcto Funcionamiento y evitar daño al Servidor.	Se realiza las acciones de limpieza y verificación de los equipos que tiene los datos para asegurar su buen funcionamiento.

Expedientes			
Medidas de seguridad físicas	**Medida**	**Finalidad**	**Descripción**
	Expedientes. Llave de acceso al área de recursos humanos en el que se encuentran.	Prevenir que cualquier persona sin autorización ingrese al área de Recursos Humanos	Sólo las personas adscritas al área tienen acceso a la llave de la oficina.

Sistema de Control de Figuras Operativas			
Medidas de seguridad físicas	**Medida**	**Finalidad**	**Descripción**
	Bitácora registro de acceso	Tener registro de los datos de la persona que accede a site y el motivo del acceso	La persona que tiene acceso se registra en una bitácora y anota el motivo por el que accede

Solicitud de ejercicio de derechos ARCO.			
Medidas de seguridad físicas	**Medida**	**Finalidad**	**Descripción**
	Acceso a Unidad administrativa.	Prevenir el acceso no autorizado al perímetro de la organización.	Las unidades administrativas cuentan con puertas de acceso con cerraduras, las llaves se encuentran bajo resguardo del titular del área administrativa. Fuera del horario oficial de labores, salvo situaciones extraordinarias, las puertas de acceso a las unidades administrativas se deben mantener cerradas bajo llave.
		Prevenir el daño o interferencia a las instalaciones.	
		Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico.	
	Seguridad física de equipos	Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico.	Los equipos de cómputo se sitúan sobre superficies fijas, mesas de trabajo y escritorios, a una altura adecuada para evitar caídas daños por estas.

			Los equipos de cómputo se ubican lejos de ventanas para evitar que objetos lanzados desde el exterior caigan sobre ellos y los dañen.
			Tanto el equipo de cómputo (soportes electrónicos) como archiveros (soportes físicos) cuentan el debido cuidado por parte del servidor público del cual se encuentran bajo resguardo.

Solicitud de acceso a la información			
	Medida	**Finalidad**	**Descripción**
Medidas de seguridad físicas	Acceso a Unidad administrativa.	Prevenir el acceso no autorizado al perímetro de la organización.	Las unidades administrativas cuentan con puertas de acceso con cerraduras, las llaves se encuentran bajo resguardo del titular del área administrativa. Fuera del horario oficial de labores, salvo situaciones extraordinarias, las puertas de acceso a las unidades administrativas se deben mantener cerradas bajo llave.
		Prevenir el daño o interferencia a las instalaciones.	
		Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico.	
	Seguridad física de equipos	Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico.	Los equipos de cómputo se sitúan sobre superficies fijas, mesas de trabajo y escritorios, a una altura adecuada para evitar caídas daños por estas.
			Los equipos de cómputo se ubican lejos de ventanas para evitar que objetos lanzados desde el exterior caigan sobre ellos y los dañen.
			Tanto el equipo de cómputo (soportes electrónicos) como archiveros (soportes físicos) cuentan el debido cuidado por parte del servidor público del cual se encuentran bajo resguardo.

B. Medidas de seguridad técnicas

Para garantizar la seguridad técnica y operatividad de los recursos tecnológicos (hardware y software) involucrados en el tratamiento de datos personales se realizan e implementan las acciones y mecanismos en cada sistema de datos personales y/o base de datos:

Certificados Enviados			
Medidas de Seguridad técnicas	**Medida**	**Finalidad**	**Descripción**
	Prevenir el acceso a los datos mediante usuario y contraseña autorizado	Limitar el acceso a los datos mediante contraseña	Solo una persona con cuenta de acceso y contraseña tiene acceso a los datos
	Instalación y actualización de software antivirus y software de protección de redes	Proteger los datos de ataques externo y de programas maliciosos	Se Instala programa de seguridad para la protección de virus y malwares que puedan dañar el equipo o los datos
	Software de copia de seguridad	Realizar una copia de seguridad de los datos.	Se instala software de copia de seguridad para el respaldo de los datos en una unidad externa.
	Usuarios y contraseñas para acceso a Base de datos de certificados enviados.	Prevenir que el acceso a los datos personales, así como a los recursos, sea por usuarios identificados y autorizados.	Usar la Base de datos de certificados enviados.
	Usuario y contraseña de acceso al correo electrónico institucional.		
	Respaldo del archivo de Excel para la BD de certificados enviados.	Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales.	

Sistema de Control de Figuras Operativas			
Medidas de Seguridad técnicas	**Medida**	**Finalidad**	**Descripción**
	Software de copia de seguridad	Realizar una copia de seguridad de los datos.	Se instala software de copia de seguridad para el respaldo de los datos en una unidad externa.
	Instalación y actualización de software antivirus	Proteger los datos de ataques externo y de programas maliciosos	Se Instala programa de seguridad para la protección de virus y malwares que puedan dañar el equipo o los datos

Solicitud de ejercicio de derechos ARCO.			
Medidas de Seguridad técnicas	**Medida**	**Finalidad**	**Descripción**
	Usuarios y contraseñas.	Prevenir el acceso a los datos personales, por usuarios no identificados y autorizados.	El equipo de cómputo asignados al servidor público cuente con contraseña de usuario.

Solicitud de acceso a la información			
Medidas de Seguridad técnicas	**Medida**	**Finalidad**	**Descripción**
	Usuarios y contraseñas.	Prevenir el acceso a los datos personales, por usuarios no identificados y autorizados.	El equipo de cómputo asignados al servidor público cuente con contraseña de usuario.

C. Medidas de Seguridad Administrativas

Políticas y procedimientos para la gestión, soporte y revisión de la seguridad de los datos personales a nivel organizacional, la identificación, clasificación y borrado seguro de los datos personales, así como la sensibilización y capacitación del personal en materia de protección de datos personales.

Certificados Enviados			
Medidas de Seguridad Administrativas	**Medida**	**Finalidad**	**Descripción**
	Política de acceso a los datos	Determinas las acciones y requisitos para dar acceso a una persona	Conocer los requisitos para solicitar una cuenta de acceso, los diferentes niveles de acceso y la responsabilidad del cuidado de los datos
	Capacitación general a los delegados para el uso de la Base de datos de certificados enviados.	Mejorar la sensibilización y capacitación del personal en materia de protección de datos personales.	Capacitar a delegados de como entrar a la Base de datos de datos de certificados enviados, así como asignar la contraseña.
	Establecimiento de políticas para el acceso a la Base de datos de certificados enviados.	Mejorar la gestión de la seguridad de los datos personales.	Definición de que usuarios pueden tener acceso a la Base de datos de certificados enviados y desde que equipo.

Expedientes			
Medidas de Seguridad Administrativas	**Medida**	**Finalidad**	**Descripción**
	Expedientes de personal	Realizar un expediente con la información personal del trabajador	Elaboración de expedientes con la información del personal, tanto personal como laboral, con la finalidad de poder consultarlo en el momento que se requiera.

Solicitud de ejercicio de derechos ARCO.			
Medidas de Seguridad Administrativas	**Medida**	**Finalidad**	**Descripción**
	Capacitación general y particular	Sensibilizar y capacitar al personal en materia de protección de datos personales. Que el personal conozca y cumpla con los principios, deberes, derechos y demás obligaciones en la materia y las sanciones en caso de incumplimiento.	Todos los empleados deben recibir una capacitación sobre aspectos generales de la ley al menos una vez por año y los nuevos colaboradores en sus primeros 90 días de entrar en funciones, conforme al programa general de capacitación para la institución.
	Establecer Políticas y procedimientos para la gestión, soporte y revisión de la seguridad de los datos personales a nivel organizacional, la identificación, clasificación y borrado seguro de los datos personales.	Delimitar las actuaciones en la gestión de los procedimientos internos. Establecer los principios que rigen el actuar de los servidores públicos de la Comisión.	Se cuentan con las disposiciones normativas siguientes: -Reglamento interior del Instituto. -Código de Conducta de los servidores públicos del Instituto. -Ley de Transparencia y Acceso a la Información Pública del estado de Campeche. -Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Campeche. -Manual de Organización -Manual de procedimientos.

Solicitud de acceso a la información			
Medidas de Seguridad Administrativas	**Medida**	**Finalidad**	**Descripción**
	Capacitación general y particular	Sensibilizar y capacitar al personal en materia de protección de datos personales. Que el personal conozca y cumpla con los principios, deberes, derechos y demás obligaciones en la materia y las sanciones en caso de incumplimiento.	Todos los empleados deben recibir una capacitación sobre aspectos generales de la ley al menos una vez por año y los nuevos colaboradores en sus primeros 90 días de entrar en funciones, conforme al programa general de capacitación para la institución.
	Establecer Políticas y procedimientos para la gestión, soporte y revisión de la seguridad de los datos personales a nivel organizacional, la identificación, clasificación y borrado seguro de los datos personales.	Delimitar las actuaciones en la gestión de los procedimientos internos. Establecer los principios que rigen el actuar de los servidores públicos de la Comisión.	Se cuentan con las disposiciones normativas siguientes: -Reglamento interior del Instituto. -Código de Conducta de los servidores públicos del Instituto. -Ley de Transparencia y Acceso a la Información Pública del estado de Campeche. -Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Campeche. -Manual de Organización -Manual de procedimientos.

XIII. Controles de identificación y autenticación de usuarios.

Las personas trabajadoras del Instituto en todo momento contar con gafetes identificativos, los cuales cuentan con los siguientes datos:

Frente:	Al reverso:
▪ Nombre completo. ▪ Número de empleado. ▪ Cargo ▪ Fotografía ▪ Área de adscripción	▪ Vigencia. ▪ Firma del Director General. ▪ Domicilio institucional. ▪ Teléfono institucional.

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

Los soportes físicos se encuentran debidamente organizados, lo cual permite identificar el tipo de información que contiene y solamente tienen acceso al tratamiento de los mismos las personas debidamente autorizadas.

Se crean copias de respaldo mediante la digitalización de los documentos quedando los datos registrados, de tal forma que la recuperación de documentos se puede dar en cualquier momento.

Certificados Enviados.
La Política o procedimiento de respaldo de datos es una vez al día y se resguarda en una unidad externa en caso de que se sufra un daño se puede recuperar la información de la unidad externa.

Sistema Expedientes.
El sistema IS-HUMA, ofrece un respaldo constante de la información que se maneja y las operaciones que se realizan, en dado caso, se contacta a la empresa proveedora para que nos brinde acceso a dicho respaldo y así recuperar los datos.

Sistema de Control de Figuras Operativas.
Nota: LOS PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS PERSONALES, está a cargo de la Unidad de Informática, y deberá registrarlo en la bitácora de respaldos, conforme lo marca el anexo (FORMATO 5).

XV. El Plan de Contingencia.

El sitio donde se encuentra la información de los sistemas de datos personales dentro de la institución, como medidas de seguridad, se encuentran resguardados dentro de un cuarto cerrado, en caso de pérdida de energía eléctrica, cuenta con dispositivos de regulación de corriente y de batería continua; cuenta con un sistema de enfriamiento para evitar las altas temperaturas, cuenta con un sistema de respaldo de información de las bases de datos en un dispositivo externo en caso de que el equipo de cómputo falle.

De igual manera, se mantiene permanentemente un constante plan de soporte técnico entre el proveedor y el Instituto, para poder proteger la información que se encuentra en los equipos de cómputo si estos llegaran a averiarse.

Las unidades administrativas en la que se encuentran los sistemas de datos personales dentro de la institución, mantienen comunicación constante con la Unidad de Informática, esto, para informar cualquier incidencia, o en caso de detectar alguna amenaza en el sistema.

No se cuenta con una Unidad Interna de Protección Civil.

Medidas de prevención y conservación de archivos
Espacios con luz natural y sin humedad.
Los muebles de archivo deben garantizar la conservación de los documentos que guardan; los documentos deben guardar uniformidad.
Evitar archivar documentación cerca de aparatos eléctricos, las instalaciones eléctricas deben estar en buenas condiciones.
Los estantes de los archivos deben de estar entre 10 y 15 cm del suelo (facilitan la limpieza y evita su vez la acumulación de humedad y proliferación de plagas).
Todos los equipos eléctricos deben quedar apagados y desconectados durante la noche o cuando no se utilicen.
Se recomienda no colocar vasos con líquido que puedan derramarse fácilmente sobre los aparatos eléctricos.

Medidas preventivas antes y después de la contingencia y/o amenazas; así como elementos para la atención ante una situación de emergencia.
No se cuenta con un protocolo, ni Unidad Interna de Protección Civil.

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

Expedientes	
Los Métodos Físicos	Los expedientes del personal se deberán conservar en el área de resguardo a menos que bajo autorización, únicamente los del personal que se da de baja en algún momento puedan enviarse a la bodega como resguardo, para futuras consultas o necesidades.

Sistema de Control de Figuras Operativas	
Los Métodos Físicos	Los expedientes del personal se deberán conservar en el área de resguardo a menos que bajo autorización, únicamente los del personal que se da de baja en algún momento puedan enviarse a la bodega como resguardo, para futuras consultas o necesidades.

Certificados Enviados	
Los Métodos Lógicos	Formateo de los discos donde se resguardan los datos personales.

Solicitud de ejercicio de derechos ARCO.	
Los Métodos Físicos	Implica la destrucción física de los documentos, a través de métodos como trituración, incineración o perforación.
Los Métodos Lógicos	Borrado de software: Utiliza programas específicos para sobrescribir los datos existentes en el medio de almacenamiento.

Solicitud de acceso a la información	
Los Métodos Físicos	Implica la destrucción física de los documentos, a través de métodos como trituración, incineración o perforación.
Los Métodos Lógicos	Borrado de software: Utiliza programas específicos para sobrescribir los datos existentes en el medio de almacenamiento.

XVII. El Plan de Trabajo.

De conformidad con lo dispuesto en el artículo 52 fracción VI de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Campeche, el responsable deberá elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, así como las medidas para el cumplimiento cotidiano de las políticas de gestión y tratamiento de los datos personales. Plan de trabajo que defina las acciones a implementar de acuerdo a los resultados del análisis de riesgos y del análisis de brecha, priorizando las medidas de seguridad más relevantes e inmediatas a establecer.

Acción	Responsable	Unidad administrativa	Plazo de tiempo	Recurso
Pérdida de suministro de energía.	Jefe del Área	Área de recursos materiales.	1 mes.	Instalación de una red de energía externa a la principal.
Espionaje remoto.	Ing. José Carlos Ramírez Uc.	Área de Mantenimiento y Desarrollo de sistema.	Permanente.	Software de monitoreo de conexiones de red.
Uso no autorizado de equipos.	Ing. Cynthia Amabilis Vivas.	Unidad de Informática.	1 mes.	

En el Sistema de figuras operativas no se tiene nivel de riesgo alto o muy alto, por lo tanto, no se aplica un plan de trabajo para tratamientos de este tipo de riesgos.

De lo anterior, se consideran los recursos designados, el personal interno y externo en la institución y las fechas establecidas para la implementación de las medidas de seguridad nuevas o faltantes.

En caso de que se identifiquen cambios en las amenazas, las vulneraciones o el impacto de los riesgos identificable, se pueden realizar actualizaciones al plan de trabajo.

XVIII. Mecanismos de monitoreo y revisión de las medidas de seguridad.

El artículo 56 fracción XVIII de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Campeche establece como una de las actividades a realizar para implementar y mantener medidas de seguridad para la protección de datos personales los mecanismos de monitoreo y revisión de las medidas de seguridad.

Monitoreo del entorno físico.
Para la atención continua de amenazas y vulnerabilidades en el entorno físico, se cuenta con personal de vigilancia en el acceso principal del edificio, control de acceso a través de bitácoras para visitantes, control de asistencia a través de huella digital, y circuito cerrado a través de cámaras de vigilancia.

Monitoreo del entorno electrónico.
Detección continua de amenazas y vulnerabilidades, se cuenta con herramientas automatizadas o programas de monitoreo.

Además del monitoreo continuo de las medidas de seguridad, para fortalecer la protección de los datos personales que resguarda este organismo; se pretende realizar una supervisión periódica de las medidas de seguridad, a través de supervisiones, las cuales pueden ser internas (desarrolladas por el Comité); a continuación, se describen los mecanismos de monitoreo y revisión de cada uno de los sistemas y/o base de datos.

Sistema de tratamiento y/o base de datos personales: Certificados Enviados	
Actividad	**Descripción**
Revisión mensual del estado del equipo que tiene los datos.	Al inicio de cada mes se realiza una revisión de la estructura de red y del equipo que contiene los datos para prevenir daño.

Sistema de tratamiento y/o base de datos personales: Expedientes	
Actividad	**Descripción**
Revisiones periódicas.	Revisar los expedientes, para verificar su contenido, si este necesita actualizarse o si existe información que ya no sea de utilidad y pueda depurarse.
Actualización de información	En el expediente deberá archivarse toda aquella nueva información del personal, a fin de mantener actualizado el expediente

Sistema de tratamiento y/o base de datos personales: Sistema de Control de Figuras Operativas	
Actividad	**Descripción**
Respaldo	Es una herramienta para resguardar una copia de los datos originales con la finalidad de disponer o recuperarlos en caso de pérdida, es un método de prevención para proteger la información capturada.

Sistema de tratamiento y/o base de datos personales: Solicitud de ejercicio de derechos ARCO.	
Actividad	**Descripción**
Informe anual.	Se realizará un informe detallado de las medidas de seguridad existentes de manera anual por parte del oficial de Datos Personales, informando al Comité de Transparencia el estado que éstas guardan, durante el mes de enero de cada año.

Sistema de tratamiento y/o base de datos personales: Solicitud de acceso a la información	
Actividad	**Descripción**
Informe anual.	Se realizará un informe detallado de las medidas de seguridad existentes de manera anual por parte del oficial de Datos Personales, informando al Comité de Transparencia el estado que éstas guardan, durante el mes de enero de cada año.

XIX. Programa General de Capacitación.

En relación al programa de capacitación, la fracción VIII del artículo 52 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Campeche señala que, para establecer y mantener las medidas de seguridad para la protección de datos personales, el responsable deberá diseñar y aplicar diferentes niveles de capacitación del personal bajo su mando, dependiendo de sus roles y responsabilidades respecto del tratamiento de los datos personales.

De acuerdo con la fracción XIX del artículo 56 de la Ley, el programa de capacitación forma parte del documento de seguridad. Se deberá diseñar e implementar programas a corto, mediano y largo plazo que tengan por objeto capacitar a los involucrados internos y externos de su organización, considerando sus roles y responsabilidades asignadas para el tratamiento y seguridad de los datos personales y el perfil de sus puestos.

Por ello, se han diseñado los programas de capacitación clasificándolos por cada uno de los sistemas de datos personales implementados dentro de la institución, con el propósito de mantener actualizados en los temas del tratamiento de datos personales.

Sistema de tratamiento y/o base de datos personales: Certificados Enviados.	
Estrategias de Capacitación	
Tipo de Capacitación	**Actividades**
Programa de capacitación a anual sobre la protección de datos personales	Realizar cada año una capacitación para todo el personal sobre la ley de protección de datos personales o en su caso cuando salga una actualización de la misma
Acciones de Capacitación a responsables de tratamiento	
Taller de capacitación periódicamente sobre la protección de datos personales	Solicitar COTAIPEC taller de capacitación de la ley de protección de datos para los administradores de base de datos

Sistema de tratamiento y/o base de datos personales: Expedientes.	
Estrategias de Capacitación	
Tipo de Capacitación	**Actividades**
Presencial (en el área)	Dar a conocer de qué manera manejar los expedientes del personal, que contienen, y en qué lugar físico en específico se encuentra.

Sistema de tratamiento y/o base de datos personales: Sistema de control de figuras operativas	
Estrategias de Capacitación	
Tipo de Capacitación	**Actividades**
Taller	Implementar un taller para capacitar a los servidores públicos que manejan datos personales.
Acciones de Capacitación a responsables de tratamiento	
Taller de capacitación y actualización en materia de protección de datos personales	Realizar anualmente una capacitación al personal respecto a sus funciones y responsabilidad en el tratamiento y seguridad de los datos personales.

Sistema de tratamiento y/o base de datos personales: Solicitud de ejercicio de derechos ARCO.	
Estrategias de Capacitación	
Tipo de Capacitación	**Actividades**
Capacitación permanente	Ofrecer cursos sobre aspectos generales de la Ley de Protección de Datos Posesión de Sujetos Obligados del Estado de Campeche.
Acciones de Capacitación a responsables de tratamiento	
Curso: Aspectos Generales de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados.	Proporciona a los servidores públicos las herramientas necesarias que les permitan mejorar la gestión de la protección de datos personales a fin de incrementar los niveles de seguridad en el tratamiento de datos personales al interior de la institución.
Lineamientos para la Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Campeche.	
Curso taller: Derechos ARCO.	
Taller: Documento de seguridad y Aviso de Privacidad Impartido por: Oficial de Protección de Datos Personales.	

Sistema de tratamiento y/o base de datos personales: Solicitud de acceso a la información	
Estrategias de Capacitación	
Tipo de Capacitación	**Actividades**
Capacitación permanente.	Ofrecer cursos sobre aspectos generales de la Ley de Protección de Datos Posesión de Sujetos Obligados del Estado de Campeche.
Acciones de Capacitación a responsables de tratamiento	
Curso: Aspectos Generales de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados.	Proporciona a los servidores públicos las herramientas necesarias que les permitan mejorar la gestión de la protección de datos personales a fin de incrementar los niveles de seguridad en el tratamiento de datos personales al interior de la institución.
Lineamientos para la Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Campeche.	
Curso taller: Derechos ARCO.	
Taller: “Documento de seguridad y Aviso de Privacidad”, impartido por: Oficial de Protección de Datos Personales.	

XX. Actualización del documento de seguridad.

El artículo 57 de la Ley de Protección de Datos Personales en Posesión de Datos Personales en Posesión de Sujetos Obligados, establece la obligación de la actualización del documento de seguridad cuando ocurran los siguientes eventos:

I. Se produzcan modificaciones sustanciales al tratamiento de datos personales que deriven en un cambio en el nivel de riesgo
II. Como resultado de un proceso de mejora continua, derivado del monitoreo y revisión del sistema de gestión;
III. Como resultado de un proceso de mejora para mitigar el impacto de una vulneración a la seguridad ocurrida, e
IV. Implementación de acciones correctivas y preventivas ante una vulneración de seguridad.

En este sentido, el Comité de Transparencia estará pendiente para la actualización de alguno de los supuestos antes citado, para, en su caso, actualizar el presente documento de seguridad.

El siguiente cuadro muestra las fechas en que se ha actualizado el documento de seguridad del IEEA:

Fecha de actualización	Motivo de la actualización
12/09/2013	Aprobación del Documento de Seguridad del IEEA.
03/12/2024	Como resultado de un proceso de mejora continua, derivado del monitoreo y revisión del sistema de gestión. Aprobado por el Comité de Transparencia del IEEA.

Anexos

ANEXO 1

FORMATO DE INGRESO/SALIDA DE EQUIPOS DE CÓMPUTO

Instituto Estatal de la Educación para los Adultos del Estado de Campeche

Número de Folio:			Fecha:	
Nombre y cargo del solicitante:				
Área de adscripción:				
Descripción del Equipo:	**Marca**	**Modelo**	**Serie**	**Número de Inventario**

Salida del Equipo de Cómputo:

Fecha:_____ Hora:_____

El bien es propiedad del IEEA Si ☐ No ☐

Nombre del responsable del equipo: _____

Motivo del préstamo: Reparación ☐ Comisión ☐ Otro:_____

Tiempo aproximado del préstamo: _____

_____ Firma del Solicitante

_____ Firma del Responsable del Equipo

Devolución del equipo de cómputo:

Fecha:_____ Hora:_____

Descripción del equipo:

_____ Firma del Solicitante

_____ Firma del Responsable del Equipo

ANEXO 2

BITÁCORA DE TRANSFERENCIAS

Instituto Estatal de la Educación para los Adultos del Estado de Campeche

Fecha	Medio	Datos Personales Transferidos	Receptor	Persona que recibe

Autorización

_____

Nombre, Cargo y Firma

Se hace de su conocimiento que esta información es considerada como confidencial, porque contiene datos personales, por lo que solicitamos darle el trato correspondiente en base a los Lineamientos para la Protección de Datos Personales del Estado de Campeche, artículos 27, 28 del Marco normativo en Materia de Transparencia y Acceso a la Información Pública, y de los artículos 1, 2 de la Ley de Protección de Datos Personales del Estado de Campeche y sus municipios.
Por lo que informamos que su uso es bajo su responsabilidad.

ANEXO 3

BITÁCORA DE ACCESO

Instituto Estatal de la Educación para los Adultos del Estado de Campeche						
Nombre y cargo de quien accede	**Área de adscripción**	**Identificación del Expediente**	**Fojas del Expediente**	**Propósito del Acceso**	**Fecha y hora de Acceso**	**Fecha y hora de Devolución**

ANEXO 4

VULNERACIONES A LA SEGURIDAD DE DATOS PERSONALES

Instituto Estatal de la Educación para los Adultos del Estado de Campeche	
Vulneración a la seguridad de datos personales	
Fecha del incidente:	
Nombre y cargo:	
Área de adscripción:	
Responsable del área:	
Sistema de tratamiento o base de datos personales vulnerada.	
Soporte de la información vulnerada	Físico ☐ Electrónico ☐ Ambos ☐
Tipo de vulneración:	☐ Pérdida o destrucción no autorizada ☐ Robo, extravío o copia no autorizada ☐ Uso, acceso o tratamiento no autorizado ☐ Daño, afectación o modificación no autorizada
Tipo de dato personal afectado:	☐ Identidad ☐ Académicos ☐ Electrónico ☐ Laboral ☐ Procedimientos administrativos o jurisdiccionales ☐ Tránsito y movimientos migratorios ☐ Biométricos ☐ Naturaleza Pública ☐ Afectivos y/o similares
_____ Nombre y Firma de quien reporta	_____ Nombre y Firma del administrador del Sistema

ANEXO 5

PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS PERSONALES

Instituto Estatal de la Educación para los Adultos del Estado de Campeche						
Área:			**Equipo:**			
			Serie:			
Nombre y cargo del responsable del equipo	**Fecha**	**Hora:**	**Tipo**			**Observaciones**
			A	**B**	**C**	

"A" RESPALDO COMPLETO: Respaldo de todos los ficheros y directorios.
"B" RESPALDO DIFERENCIAL: Respaldo de todos los ficheros y directorios modificados desde el último respaldo completo.
"C" RESPALDO INCREMENTAL: Respaldo de todos los ficheros y directorios modificados desde el último respaldo.