

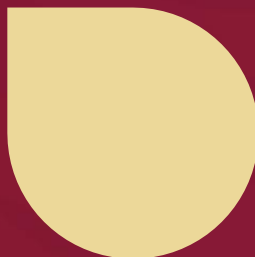
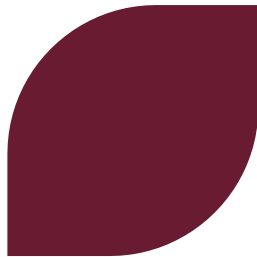


COLIMA
Gobierno del Estado



Instituto Colimense
de las Mujeres

DOCUMENTO DE SEGURIDAD PARA LA PROTECCIÓN DE LOS DATOS PERSONALES DEL INSTITUTO COLIMENSE DE LAS MUJERES (ICM)



INTRODUCCIÓN

El Instituto Colimense de las Mujeres, como organismo público descentralizado de la Administración Pública Estatal, reconoce que la información constituye uno de sus activos institucionales más importantes, particularmente aquella relacionada con los datos personales y datos personales sensibles de las mujeres usuarias de los servicios institucionales, personas servidoras públicas, proveedoras, proveedores y demás personas físicas con quienes mantiene relación derivada del ejercicio de sus atribuciones.

En este sentido, el Instituto Colimense de las Mujeres se encuentra obligado a garantizar la protección de los datos personales que obran en su posesión, mediante la implementación de medidas de seguridad administrativas, físicas y técnicas que permitan asegurar su confidencialidad, integridad y disponibilidad, conforme a lo dispuesto por la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Colima y demás disposiciones aplicables.

Las actividades sustantivas del Instituto implican el tratamiento de información altamente sensible relacionada con la atención de mujeres en situación de violencia, atención psicológica, trabajo social, asesoría jurídica, refugio especializado, atención a niñas, niños y adolescentes, así como información laboral, administrativa y financiera de las personas servidoras públicas adscritas al organismo.

Por lo anterior, resulta indispensable establecer mecanismos formales que permitan identificar los riesgos asociados al tratamiento de los datos personales, implementar medidas de protección adecuadas, establecer procedimientos de respuesta ante incidentes de seguridad y promover una cultura institucional de protección de datos personales.

El presente Documento de Seguridad constituye el instrumento mediante el cual el Instituto Colimense de las Mujeres describe las medidas de seguridad administrativas, físicas y técnicas implementadas para proteger los datos personales bajo su resguardo, de conformidad con lo previsto en los artículos 32 y 33 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Colima.

Contenido

INTRODUCCIÓN 2

1.- GLOSARIO.....4

2.- INVENTARIO DE DATOS Y SISTEMAS DE TRATAMIENTO. 8

3.- FUNCIONES Y OBLIGACIONES DE LAS PERSONAS QUE INTERVIENEN EN EL
TRATAMIENTO DE DATOS PERSONALES 10

4.- ANÁLISIS DE RIESGOS..... 11

5.- ANÁLISIS DE BRECHA..... 16

6.- PLAN DE TRABAJO.....18

7.- MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD. 19

8.- PROGRAMA GENERAL DE CAPACITACIÓN..... 25

1.- 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.
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.
Contraloría	Contraloría General del Gobierno del Estado de Colima.
Ley	Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Colima.
Ley de Transparencia	Ley de Transparencia y Acceso a la Información Pública del Estado de Colima.
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 la protección, confidencialidad, disponibilidad e integridad de los datos personales.
Medidas de seguridad administrativas	Políticas y procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, la identificación, clasificación y borrado seguro de la información, así como la sensibilización, formación y capacitación del personal en materia de protección de datos personales.
Medidas de seguridad físicas	Conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento.
Medidas de seguridad técnicas	Conjunto de acciones y mecanismos que se valen de la tecnología relacionada con hardware y software para proteger el entorno digital de los datos personales y recursos involucrados en su tratamiento.
N/A	No aplica.

Responsable	Los sujetos obligados definidos en el artículo 3, fracción XXIX, de la Ley de protección de datos local, 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	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.

Diagnóstico de la institución.

El Instituto Colimense de las Mujeres tiene por objeto promover, proteger y garantizar los derechos humanos de las mujeres en el Estado de Colima, así como implementar políticas públicas orientadas a la igualdad sustantiva, prevención y atención de la violencia de género.

Para el cumplimiento de sus atribuciones, el Instituto realiza el tratamiento de datos personales y datos personales sensibles a través de diversas áreas administrativas y operativas.

Las áreas identificadas que realizan tratamiento de datos personales son:

- Dirección General.
- Coordinación Administrativa.
- Recursos Humanos.
- Contabilidad.
- Jurídico.
- Unidad de Transparencia.
- Psicología.
- Trabajo Social.
- Centros LIBRE.
- Refugio Especializado.
- Archivo Institucional.
- Comunicación Social.
- BACOLVIM.

Derivado de la naturaleza de los servicios que presta el Instituto, se identificó la existencia de datos personales sensibles relacionados con:

- Estado de salud.
- Información psicológica.
- Violencia de género.
- Información de niñas, niños y adolescentes.
- Datos de origen étnico.
- Situaciones familiares y socioeconómicas.

Medidas de seguridad para la protección de los datos personales, características y fundamentación.

La práctica internacional en la seguridad y la protección de los datos personales, nos lleva a tener cada vez más, y de una manera exhaustiva, definidas las medidas de seguridad técnicas, físicas y administrativas en los sistemas de tratamiento de los datos personales de los diferentes niveles en la administración pública Federal, Estatal y Municipal.

La Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados, así como nuestra ley armonizada para el Estado de Colima en dichos preceptos normativos, definen dichas medidas de seguridad en su artículo 3, fracciones XX, XXI, XXII y XXIII; sin embargo es importante aclarar las diferencias que existen entre estas medidas de seguridad administrativas, físicas y técnicas para tener en claro los elementos teóricos al momento de esbozar el fundamento y la estructura de este documento.

a) Las medidas de seguridad **Administrativas** son aquellas que deben implementarse para la consecución de los objetivos contemplados en los siguientes apartados:

- **Política de seguridad.** Definición de directrices estratégicas en materia de seguridad de activos, alineadas a las atribuciones de las dependencias o entidades. Incluye la elaboración y emisión interna de políticas, entre otros documentos regulatorios del sujeto obligado.
- **Cumplimiento de la normatividad.** Los controles establecidos para evitar violaciones de la normatividad vigente, obligaciones contractuales o la política de seguridad interna. Abarca, entre otros, la identificación y el cumplimiento de requerimientos tales como la legislación aplicable.
- **Organización de la seguridad de la información.** Establecimiento de controles internos y externos a través de los cuales se gestione la seguridad de activos. Considera, entre otros aspectos, la organización interna, que a su vez se refiere al compromiso de la alta dirección y la designación de responsables, entre otros objetivos; asimismo, considera aspectos externos como la identificación de riesgos relacionados con terceros.

- **Clasificación y control de activos.** Establecimiento de controles en materia de identificación, inventario, clasificación y valuación de activos conforme a la normatividad aplicable.

- **Seguridad relacionada a los recursos humanos.** Controles orientados a que el personal conozca el alcance de sus responsabilidades respecto a la seguridad de activos, antes, durante y al finalizar la relación laboral.

- **Administración de incidentes.** Implementación de controles enfocados a la gestión de incidentes presentes y futuros que puedan afectar la integridad, confidencialidad y disponibilidad de la información. Incluye temas como el reporte de eventos y debilidades de seguridad de la información.

- **Continuidad de las operaciones.** Establecimiento de medidas con el fin de contrarrestar las interrupciones graves de la operación y fallas mayores en los sistemas de información. Incluye planeación, implementación, prueba y mejora del plan de continuidad de la operación del sujeto obligado.

b) Las medidas de seguridad **Físicas** atañen a las acciones que deben implementarse para contar con:

- **Seguridad física y ambiental.** Establecimiento de controles relacionados con los perímetros de seguridad física y el entorno ambiental de los activos, con el fin de prevenir accesos no autorizados, daños, robo, entre otras amenazas. Se enfoca en aspectos tales como los controles implementados para espacios seguros y seguridad del equipo.

c) Las medidas de seguridad **Técnicas** son las aplicables a sistemas de datos personales en soportes electrónicos, servicios e infraestructura de telecomunicaciones y tecnologías de la información, entre otras, se prevén las siguientes acciones:

- **Gestión de comunicaciones y operaciones.** Establecimiento de controles orientados a definir la operación correcta y segura de los medios de procesamiento de información, tanto para la gestión interna como la que se lleva a cabo con terceros. Incluye, entre otros aspectos, protección contra código malicioso y móvil, copias de seguridad, gestión de la seguridad de redes y manejo de medios de almacenamiento.

- **Control de acceso.** Establecimiento de medidas para controlar el acceso a la información, activos e instalaciones por parte de los responsables autorizados para tal fin, considerando en ello, la protección contra la divulgación no autorizada de información. Abarca, entre otros temas, gestión de acceso de los usuarios, control de acceso a redes, control de acceso a sistemas operativos y control de acceso a las aplicaciones y a la información.

- **Adquisición, desarrollo, uso y mantenimiento de sistemas de información.** Integración de controles de seguridad a los sistemas de información, desde su adquisición o desarrollo, durante su uso y mantenimiento, hasta su cancelación

o baja definitiva. Considera procesamiento adecuado en las aplicaciones, controles criptográficos y seguridad de los archivos de sistema, entre otros.

Tipo de soportes: físicos y electrónicos.

Es importante explicar la diferencia entre un soporte físico y un soporte electrónico, debido a que las medidas de seguridad que el sujeto obligado implemente para cada sistema de datos personales, están estrechamente relacionadas con el tipo de soportes utilizados. Como definiciones aceptadas, entre organismos nacionales e internacionales en materia de protección de datos personales, tenemos las siguientes:

Soportes físicos.

Son los medios de almacenamiento inteligibles a simple vista, es decir, que no requieren de ningún aparato que procese su contenido para examinar, modificar o almacenar los datos; es decir, documentos, oficios, formularios impresos llenados “a mano” o “a máquina”, fotografías, placas radiológicas, carpetas, expedientes, entre otros.

Soportes electrónicos.

Son los medios de almacenamiento inteligibles 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 (CD y DVD), discos magneto-ópticos, discos magnéticos (flexibles y duros) y demás medios de almacenamiento masivo no volátil. Una vez explicado lo anterior, es preciso señalar que el sujeto obligado deberá identificar el tipo de soporte en el que residen los datos personales de cada uno de los sistemas que posee con el propósito de corroborar que las medidas de seguridad implementadas sean aplicables a cada caso. Por tanto, en el Documento de seguridad deberá constar si los datos personales del sistema residen en: i) Soporte físico; ii) Soporte electrónico; o iii) Ambos tipos de soportes.

2.- INVENTARIO DE DATOS Y SISTEMAS DE TRATAMIENTO.

El inventario de datos personales y de los sistemas de tratamiento es una herramienta primaria en la identificación de aquellos datos que se recaban y se gestionan al interior de la institución, así como también de los controles mínimos de seguridad para su tratamiento y por supuesto el responsable de administrar los mismos. Por cada uno de los datos personales identificados, se debe identificar el sistema de tratamiento en el cual están siendo gestionados, si es físico o electrónico, como es el caso de los soportes físicos tales como expedientes, archiveros, gavetas, anaqueles y bodegas en los cuales se procesan y almacenan dichos datos, también en el mismo sentido se deben identificar los soportes electrónicos, tales como aplicaciones, bases de datos, unidades de almacenamiento, equipos y toda aquella infraestructura tecnológica en los cuales se procesan y almacenan dichos datos. En este sentido, y toda vez que ha sido plenamente identificado el nivel de riesgo por

tipo de dato que se trata aquí en el Instituto, se estructura la información en un esquema de inventario que cuenta con las columnas de requerimiento de información necesarias para tener plenamente identificado el tipo de dato personal que manejamos y sus características normativas principales, así como el tipo de Sistema desde el cual se les da tratamiento. Los formatos de Inventarios de Datos Personales y Sistemas de Tratamiento de cada una de las áreas que lo reportaron, podrán ser consultadas de manera anexa al presente documento.

El Instituto Colimense de las Mujeres administra información contenida tanto en soportes físicos como electrónicos.

Sistemas de Tratamiento Físicos

- Expedientes laborales.
- Expedientes jurídicos.
- Expedientes psicológicos.
- Expedientes de trabajo social.
- Expedientes del refugio especializado.
- Expedientes administrativos.
- Archivo institucional.

Sistemas de Tratamiento Electrónicos

- Plataforma BACOLVIM.
- Cuentas institucionales de Gmail.
- Google Drive Institucional.
- Equipos de cómputo institucionales.
- Disco duro externo para respaldos.

Clasificación de Datos Personales Tratados

- a)** Datos de identificación:
Nombre, domicilio, teléfono, CURP, RFC, firma y correo electrónico.
- b)** Datos patrimoniales:
Información bancaria y financiera.
- c)** Datos laborales:
Expedientes laborales y administrativos.
- d)** Datos jurídicos:
Expedientes de representación y asesoría jurídica.
- e)** Datos sensibles:
Información psicológica, médica, familiar, socioeconómica, violencia de género, niñas, niños y adolescentes y origen étnico.

3.- FUNCIONES Y OBLIGACIONES DE LAS PERSONAS QUE INTERVIENEN EN EL TRATAMIENTO DE DATOS PERSONALES

Con fundamento en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Colima, las personas servidoras públicas del Instituto Colimense de las Mujeres que intervienen en cualquier etapa del tratamiento de datos personales deberán observar en todo momento los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad.

Para efectos del presente Documento de Seguridad, se identifican los siguientes responsables:

Titular del Instituto Colimense de las Mujeres

Nombre: Mtra. Erika Judith Torres Guzmán

Funciones:

- Autorizar las acciones institucionales en materia de protección de datos personales.
- Promover la implementación de medidas de seguridad administrativas, físicas y técnicas.
- Supervisar el cumplimiento de las obligaciones institucionales en materia de protección de datos personales.
- Autorizar la actualización del Documento de Seguridad.

Responsable de Protección de Datos Personales

Nombre: Licda. Janeth Adriana Castro Cisneros

Funciones:

- Coordinar la implementación de medidas de seguridad.
- Supervisar el cumplimiento de la normatividad aplicable.
- Coordinar acciones de prevención y atención de incidentes.
- Llevar el control de inventarios de sistemas de tratamiento.
- Participar en la actualización periódica del Documento de Seguridad.

Responsable Jurídico

Nombre: Licda. Andrea Leticia Silva Castro

Funciones:

- Brindar asesoría jurídica en materia de protección de datos personales.
- Emitir opiniones respecto de vulneraciones de seguridad.
- Participar en procedimientos derivados de incidentes de seguridad.

- Elaborar instrumentos jurídicos relacionados con transferencias de datos personales.

Responsable de Tecnologías de la Información

Nombre: Ing. César Augusto Matus Zavala

Funciones:

- Administrar la infraestructura tecnológica institucional.
- Implementar controles de acceso a sistemas informáticos.
- Supervisar respaldos y recuperación de información.
- Participar en la atención de incidentes tecnológicos.
- Mantener actualizadas las medidas técnicas de seguridad.

Responsable de la Unidad de Transparencia

Nombre: Mtro. Alfonso Emmanuel Parra Valdez

Funciones:

- Coordinar la atención de solicitudes de derechos ARCO.
- Asesorar a las áreas administrativas en materia de protección de datos personales.
- Promover la capacitación institucional.
- Coordinar la elaboración y actualización del Documento de Seguridad.
- Fungir como enlace institucional con la Contraloría General del Estado.

Obligaciones Generales del Personal

Todas las personas servidoras públicas que tengan acceso a datos personales deberán:

- Utilizar la información únicamente para el cumplimiento de sus funciones.
- Guardar confidencialidad respecto de la información a la que tengan acceso.
- Abstenerse de divulgar datos personales sin autorización legal.
- Informar inmediatamente cualquier incidente de seguridad.
- Cumplir las medidas de seguridad establecidas en el presente documento.

4.- ANÁLISIS DE RIESGOS

El análisis de riesgos en el tratamiento de los datos personales, viene establecido en la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados, y mandatado de igual forma en el artículo 30, fracción IV de nuestra Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados para el Estado de Colima (LPDPPSOEC). En este sentido, el presente análisis, se sustenta en la Metodología BAA (Beneficio, Accesibilidad y Anonimidad del atacante); esta metodología en particular, contempla tres factores que en conjunto determinan el riesgo latente de los datos personales:

- **Beneficio, factor** que deriva en el nivel de **riesgo por tipo de dato**, determinado por el riesgo inherente del dato y el volumen de titulares de las que se tratan datos.
- **Accesibilidad, factor** que determina el nivel de **riesgo por tipo de acceso**, es decir, el número de accesos potenciales a los datos.
- **Anonimidad, factor** que determina el nivel de **riesgo por tipo de entorno** desde el que se tiene acceso a los datos.

Como se podrá observar, la escala de ponderación y análisis de **Nivel < > (menor que – mayor que)** en la metodología BAA (Beneficio, Accesibilidad y Anonimidad), se esquematiza mediante la categorización de números del **1 al 5**, en donde **1** implica **bajo** y **4, 5** implica **Reforzado**, dependiendo del tipo dato, el nivel de riesgo inherente, la anonimidad del atacante y la cantidad de titulares de datos personales que está en juego; enfatizando la intensidad de dicha categorización numérica con la siguiente coloración específica:

FACTOR Beneficio: El nivel de riesgo por tipo de dato

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

Clasificación de los datos personales en el Instituto Colimense de las Mujeres.

En el caso del Instituto Colimense de las Mujeres, derivado del análisis y estructuración de los inventarios de datos personales por área ejecutiva y administrativa, se determinó que existen seis tipos de datos personales que se gestionan al interior de esta institución, que son: Ubicación, Patrimoniales, Autenticación, Jurídicos, Tarjeta Bancaria, Personales de Identificación; en este sentido, como se puede constatar, bajo la valoración esquemática de la Metodología BAA, estos tipos de datos personales encuadran en los supuestos de **Datos con riesgo inherente medio** respectivamente, bajo la consideración referida supralíneas, que atiende principalmente al tipo de dato gestionado, el riesgo y el número de titulares de datos personales que se posea. Así entonces, el esquema de valoración de las dos categorías de datos expresadas quedaría de la siguiente manera:

Identificación de tipos de datos y de nivel de riesgo inherente en el Instituto Colimense de las Mujeres.

Tipo de Dato	Nivel de riesgo inherente
Ubicación	Medio
Patrimoniales	Medio
Autenticación	Medio
Jurídico	Medio
Tarjeta Bancaria	Medio
Personales de Identificación	Medio

Identificación de riesgo por tipo de dato.

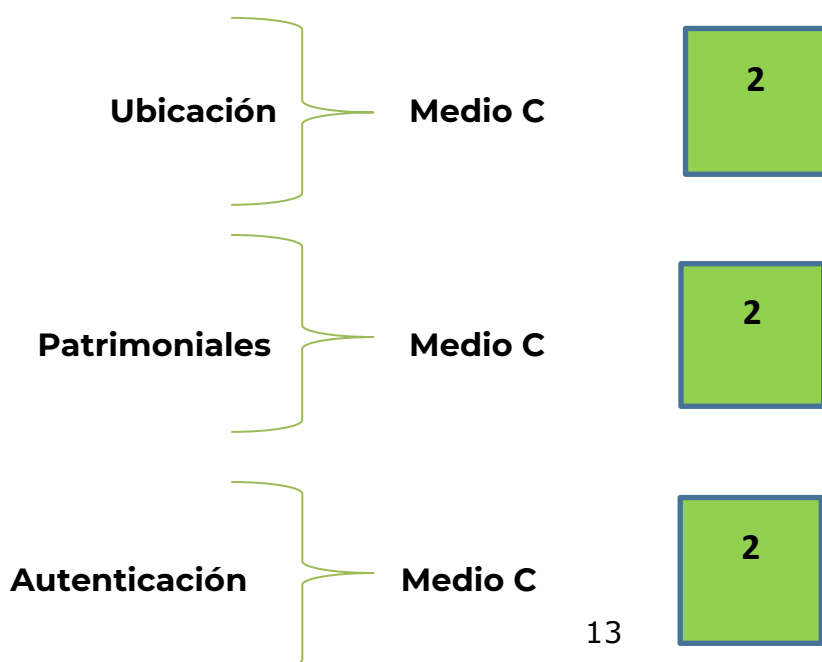
Tipo de Dato	Nivel de Riesgo Inherente	Volumen de Titulares
Ubicación	Medio	<50k
Patrimoniales	Medio	<50k
Autenticación	Medio	<50k
Jurídico	Medio	<50k
Tarjeta Bancaria	Medio	<50k
Personales de Identificación	Medio	<50k

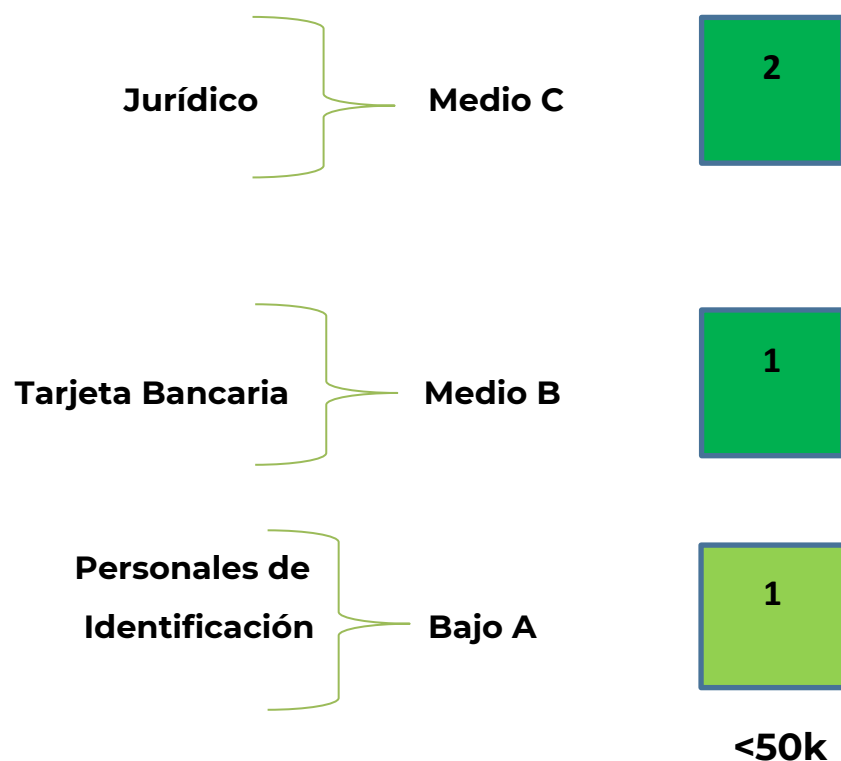
Identificación del nivel de riesgo por tipo de dato.

Al definir el nivel de riesgo inherente por cada tipo de dato y el volumen de titulares, se podrá identificar el nivel de *riesgo por tipo de dato* que se trata en la institución. Como se mencionaba supralíneas, se han establecido cinco niveles posibles con valor numérico del **1 al 5**, donde **1** es el nivel **más bajo** y **5** el **más alto**, en este sentido, la esquematización del tipo de dato y tipo de riesgo gestionado en el Instituto, se describe de la siguiente manera:

TIPO DE DATO

RIESGO INHERENTE





De lo anterior, se precisa entonces, de acuerdo a la misma clasificación en la Metodología BAA, que el Riesgo por tipo de dato es de **Nivel 2**, el cual ocurre cuando:

- El nivel de riesgo inherente de los datos personales sea medio y se tengan hasta cincuenta mil (50,000) personas
- El nivel de riesgo inherente de los datos personales sea alto y se tengan hasta cinco mil (5,000) personas.

FACTOR de Accesibilidad: El nivel de riesgo por tipo de acceso

Una vez obtenido el factor **Beneficio**, es decir el nivel de *riesgo por tipo de dato*, es necesario identificar el nivel de *riesgo por tipo de acceso*. Se realiza determinando la cantidad de accesos potenciales a los datos personales que se pretende proteger, es decir, definiendo cuántas personas tienen la posibilidad de acceder a la información en un intervalo de tiempo, por ejemplo, durante 24 horas. Para este parámetro, entre mayor sea la accesibilidad, mayor riesgo existe para la información.

A este respecto, en el caso del Instituto, se puede tomar como referencia la jornada laboral de 8 horas. Para este parámetro, entre mayor sea la accesibilidad a las bases de datos que contengan datos personales por parte del personal de la institución o ajenos a la misma, mayor riesgo existe para dicha información; de ahí la importancia del diagnóstico inicial institucional, para determinar a través de la identificación de las bases de datos que resguardan datos personales y el control de inventario de los mismos, el personal que estará cargo de dicha responsabilidad de conformidad con los principios y deberes que nos marca la ley local en la materia.

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

Nivel de riesgo por tipo de acceso en el Instituto Colimense de las Mujeres:

	Número de personas que acceden a los Datos Personales	Cantidad de Acceso a los Datos Personales	Tipo de riesgo Inherente
ACCESIBILIDAD	>20 <200	>20 >200	Medio

FACTOR de Anonimidad: El nivel de riesgo por tipo de entorno.

Después de obtener el factor **Accesibilidad**, se debe identificar qué tan anónimos son los accesos a la información; es decir, el nivel de *riesgo por tipo de entorno*. Este factor representa el nivel de percepción que se tiene de que un atacante potencial provoque consecuencias negativas para la institución, en caso de acceder o hacer uso no autorizado de los datos personales que se tratan.

En la siguiente tabla se listan los entornos de acceso, de igual forma en una escala del 1 al 5, en donde **1** implica **baja anonimidad** y **5** **mayor anonimidad** del atacante, es decir, entre más anónimo pueda ser un atacante, mayor confianza obtiene para intentar vulnerar la seguridad.

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

Nivel de riesgo por tipo de entorno en el Instituto Colimense de las Mujeres.

ENTORNO	NIVEL DE ANONIMIDAD
FÍSICO	1 (Bajo)
RED INTERNA	1 (Medio)

En este contexto, en relación al nivel de riesgo por tipo de entorno, en ámbito del entorno Físico, se cuentan con las medidas de seguridad físicas básicas para proteger la información y los activos que se administran, con los parámetros de mejora correspondientes y descritas en el propio apartado de medidas de seguridad que a continuación se presenta. A su vez, en el ámbito del entorno de Red Interna, se cuenta con las medidas de seguridad técnicas básicas, para evitar en la medida de lo posible filtraciones anónimas o pérdida de la información, parámetros perfectibles que en el siguiente apartado se describen.

Identificación de medidas de seguridad.

Una vez obtenido el nivel que le corresponde a cada factor de riesgo, se deben identificar las medidas de seguridad aplicables a la institución. A este respecto, antes de abordar el esquema que describe las medidas Físicas, Técnicas y Administrativas de la Instituto, vale la pena realizar una concatenación funcional con la explicación y descripción de los elementos generales que contempla un análisis de brecha; el cual, junto con los elementos examinados y valorados en el análisis de riesgos, nos permiten explicar cuáles son las medidas de seguridad con las que cuenta actualmente nuestra institución, en que parámetro se realiza cada medida abordada, y en el caso de que aún no se realice, la meta temporal definida para su realización.

5.- ANÁLISIS DE BRECHA.

En este análisis, nos debemos enfocar, al igual que en el análisis de riesgos, en la seguridad de los datos personales recabados y gestionados por cada área del Instituto que tenga la atribución para su tratamiento. Lo anterior, se hace realizando un diagnóstico de las prácticas de seguridad de la información con las que cuenta en ese momento el sujeto obligado y las que deberían de tenerse con base a las mejores prácticas. Algunos de los aspectos a contemplar y evaluar en el análisis de brecha son los siguientes:

- **Seguridad institucional:**

Control de la información compartida con terceros; a través de la identificación de los inventarios de datos personales por área, el responsable, y la aplicación de las medidas de seguridad para su protección.

- **Activos del responsable:**

Entendiéndose por activo, el tipo de dato recabado y gestionado en la institución, de los cuales se asignan responsabilidades para su protección y clasificación.

- **Seguridad en recursos humanos:**

Cuidar la seguridad de los recursos humanos previo a la contratación; cláusula contractual que comprometa y obligue al empleado a respetar el deber de seguridad y confidencialidad de los datos personales que gestiona.

- **Seguridad física y ambiental:**

Áreas seguras y protección de equipamiento, especificadas en las medidas físicas para la protección de los datos personales.

- **Operación, procedimientos y comunicación:**

Parte fundamental en desarrollo e implementación del Sistema de Gestión y el Programa de Protección de Datos Personales en su caso; herramientas que se pueden desprender del propio documento de seguridad, con el cual comparten elementos.

- **Cumplimiento con leyes y lineamientos:**

Todas las herramientas y elementos de control propuestos están de conformidad a lo mandado por la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados, y lo conducente a nuestra ley local.

- **Control de acceso a la información:**

Derechos y control de acceso a aplicaciones, redes y sistemas operativos al interior de la Universidad, especificados en las medidas técnicas de seguridad.

- **Incidentes de seguridad de información:**

Se cuenta con los procedimientos y formatos establecidos para identificar y mitigar algún incidente de seguridad en la institución.

Lista de medidas administrativas para nivel Medio-Alto.

Tipo de medida	Categoría	Estado actual	Estado objetivo	Acción correctiva	Prioridad
Administrativa	Prevención de pérdida de datos	Procedimientos inexistentes	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.	Mantener un procedimiento de monitoreo constante.	Alta
Administrativa	Concienciación, educación y entrenamiento en seguridad de la información	Programa inexistente de capacitación sobre protección y seguridad de datos personales dirigido al personal del Instituto.	Que el personal y, cuando corresponda, terceros reciban capacitación periódica acorde con sus funciones y con los riesgos de la información que manejan.	Elaborar un calendario anual de capacitación que incluya manejo seguro de expedientes, confidencialidad, reporte de incidentes y protección de datos personales; conservar listas de asistencia y constancias.	Media

Lista de medidas técnicas para nivel Alto.

Tipo de medida	Categoría	Estado actual	Estado objetivo	Acción correctiva	Prioridad
Técnica	Respallos de información	Procedimientos inexistentes	Contar con copias de respaldo periódicas de la información y aplicaciones relevantes, protegidas con medidas equivalentes a las de la información original, y cuya recuperación se pruebe.	Documentar con el área de tecnologías el alcance y la frecuencia de los respaldos; restringir el acceso a las copias y programar pruebas de restauración, registrando resultados y acciones correctivas.	Alta
Técnica	Identificación y autenticación de usuarios	Está pendiente integrar evidencia de que cada persona usuaria de los sistemas que contienen datos personales cuenta con una cuenta individual y permisos acordes con sus funciones.	Que cada persona utilice un identificador único y un mecanismo de autenticación; que los accesos se otorguen, revisen y retiren conforme a sus funciones y a los movimientos de personal.	Elaborar o actualizar el inventario de cuentas y permisos; revisar periódicamente los accesos con las áreas responsables y solicitar la baja o modificación de cuentas cuando cambien las funciones o concluya la relación laboral.	Alta

Lista de medidas físicas para nivel Alto.

Tipo de medida	Categoría	Estado actual	Estado objetivo	Acción correctiva	Prioridad
Físicas	Perímetro de seguridad física	Está pendiente identificar y documentar los espacios y archiveros donde se resguardan expedientes físicos con datos personales, así como los controles de acceso existentes.	Restringir el acceso a expedientes y áreas de resguardo mediante cerraduras, llaves u otros mecanismos, permitiéndolo únicamente a personal autorizado.	Elaborar un inventario de los espacios y muebles de archivo; definir quién puede acceder; asignar y controlar llaves o mecanismos de acceso y revisar periódicamente que las medidas funcionen.	Alta
Físicas	Registro de auditoría de acceso físico	Está pendiente confirmar si se registran los accesos de personal o visitantes a las áreas donde se resguarda información personal, incluyendo el motivo de ingreso.	Mantener un registro de acceso que permita identificar quién ingresó, cuándo y con qué propósito a las áreas de resguardo de información.	Implementar una bitácora para las áreas identificadas que registre fecha, hora, nombre de la persona, área que visita y motivo de acceso; designar a quien supervisará y resguardará la bitácora.	Media

6.- PLAN DE TRABAJO.

Mecanismos de monitoreo y revisión de las medidas de seguridad

En necesario planear y señalar las acciones que se tomarán en cuenta para mantener actualizadas las medidas de seguridad físicas, técnicas y administrativas que identificamos y analizamos en el análisis de riesgo y de brecha, describiendo la forma en que se llevarán a cabo dichas acciones y la temporalidad que tendrán **conforme**

a la tabla de análisis de brecha propuesta en la guía.

De manera destacada, se deben describir aquellas que no se lleven a cabo o que se consideren faltantes para la seguridad física, técnica y administrativa de los datos personales de la institución, del listado de las medidas de seguridad identificadas en el Anexo 2. Listado de Medidas de Seguridad ATF.

Para lo anterior, se debe implementar un Plan de Trabajo, señalando como control la medida de seguridad faltante, y como parámetro, la acción que se realizará para subsanarlo.

7.- MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD.

Procedimiento de respaldo y recuperación de datos personales.

Ante algún incidente o imprevisto por causas internas o externas a la institución relacionados al Software y Hardware de los sistemas informáticos que se manejan; se hace necesario un respaldo de información bien organizado y estructurado que nos permita volver a acceder a nuestros documentos para continuar trabajando con la mayor velocidad y eficiencia posibles; evitar que información importante se pierda y con ello años de trabajo, como se da el caso, cuando se daña un disco duro. A este respecto, se presenta en el siguiente esquema, los procedimientos de respaldo y recuperación implementados en el Instituto, que conforman el plan de acción en la intervención ante alguna contingencia.

Respaldo y recuperación de datos personales en entornos informáticos, Software y Hardware.

Tipo de soporte	Descripción	Procedimiento de Respaldo
FÍSICO	Discos duros Equipos de Cómputo	1.- Cada área cuenta con un medio de almacenamiento con capacidad de un terabyte para respaldo. 2.- Se realizan respaldos mensuales y llevan un control calendarizado.
ELECTRÓNICO	Correos electrónicos	1.- Análisis semestral para baja de correos electrónicos de trámite y spam. 2.- Revisión de capacidad de almacenaje de la bandeja de entrada. 3.- Respaldo semestral de correos electrónicos de trámite vigentes.

Plan de respaldo y recuperación de información.

A continuación, se esbozan los rubros que constituyen la estructura y definición de lo que implica el Plan de respaldo y recuperación de información al interior del Instituto, que se deben de tomar en cuenta, identificando primeramente el tipo de

transferencias que se realizan a nivel institucional, los controles y mecanismos para garantizar su seguridad, para posteriormente determinar si se realizan o no al interior de esta institución.

1.- Controles y mecanismos de seguridad para las transferencias.

Toda transferencia deberá formalizarse mediante la suscripción de cláusulas contractuales, convenios de colaboración o cualquier otro instrumento jurídico, de conformidad con la Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados para el Estado de Colima y de más normatividad aplicable; lo cual permite demostrar el alcance del tratamiento de los datos personales, así como las obligaciones y responsabilidades asumidas por las partes, exceptuando las realizadas entre responsables en cumplimiento de una disposición legal o en el ejercicio de sus atribuciones.

En el caso del Instituto, no se realiza ningún tipo de transferencia de datos personales, salvo petición debidamente fundada y motivada.

2.- Transferencias mediante el traslado de soportes físicos.

Ante una transferencia de información que contenga datos personales o confidenciales mediante el traslado de soportes físicos, la seguridad consiste en la aplicación de barreras físicas, y procedimientos de control como medidas de prevención, ante amenazas a dichos recursos e información confidencial, derivadas de omisiones a la protección de los mismos, accidentes o causas fortuitas.

En el caso de este Instituto no se realiza ningún tipo de transferencia mediante el traslado de soportes físicos.

3.- Transferencias mediante el traslado físico de soportes electrónicos.

En esta modalidad se trasladan físicamente para entregar al destinatario los datos personales en archivos electrónicos contenidos en medios de almacenamiento inteligibles sólo mediante el uso de algún aparato con circuitos electrónicos que procese su contenido para examinar, modificar o almacenar los datos. Al realizar transferencias físicas de soportes electrónicos se deberá considerar lo dispuesto en Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados para el Estado de Colima y de más normatividad aplicable; como ejemplo son: Los oficios de comisión para el personal autorizado y asegurar que la entrega sea a los titulares de la información o a personal autorizado para recibirla, los medios para garantizar la confidencialidad de la información, utilizar las leyendas de clasificación, registro en bitácoras de transferencia, cifrar la información, utilizar contraseñas de acceso a la misma, entre otras.

En el caso de la Instituto, no se realiza ningún tipo de transferencias mediante el traslado físico de soportes electrónicos.

4.- Transferencias mediante el traslado sobre redes electrónicas.

En esta modalidad se transmiten los datos personales en archivos electrónicos

mediante una red electrónica. Por ejemplo, cuando un archivo electrónico con un listado de beneficiarios se envía de una dependencia a otra por Internet. En el caso del Instituto, no se realiza ningún tipo de transferencia mediante el traslado en relación a las redes electrónicas.

Controles de Identificación y Autenticación de Usuarios.

Para cumplir con este objetivo, a continuación, se señala y se detalla la forma en que se identifica al personal del Instituto, así como la forma en que se autentifica a cada uno.

1.- Los empleados del Instituto deben portar en todo momento su identificación institucional que cuenta con la siguiente información:

Al frente:

- Nombre
- Cargo

Al reverso:

- Vigencia
- Número de Control
- Firma del Titular de la Institución
- Domicilio de la Institución
- Teléfono de la Institución

Identificación y registro de personas que ingresan al Instituto Colimense de las Mujeres.

Es importante tener un control ordenado y estructurado de las personas que ingresan a diario a la institución por diversos asuntos relacionados o no a las atribuciones normativas del mismo. En este sentido, se detalla la forma en que se registra a toda persona que ingresa a nuestras instalaciones:

- Personal, con libreta de registro con las siguientes columnas:
 - Nombre de la personal que ingresa
 - Institución
 - Asunto
 - Hora
 - Firma
- Puerta de cristal, previo al ingreso del edificio.
- Personal del Instituto, designado a funciones de Oficialía de Partes recibiendo a la documentación y las personas que ingresan.

Técnicas de Supresión y Borrado Seguro de Datos Personales.

No.	Criterios a considerar	Especificación
1	Comité de valoración	De conformidad con la normatividad aplicable a la materia de archivos que así lo establece, se deberá emitir un dictamen de baja y supresión de la información contenida en soportes físicos y electrónicos, que sustente el análisis fundado y motivado de la

		eliminación de dicha información de manera segura.
2	Formateo de nivel bajo	Técnica que será utilizada por el personal de la Coordinación de Informática, para la supresión y borrado seguro de la información que contenga datos personales.

Manejo de Incidentes de Seguridad de los Datos Personales.

Gestión de vulneraciones y Plan de respuesta.

Un incidente de seguridad es un riesgo materializado, en este sentido, la gestión de incidentes es el proceso de planeación, comunicación y capacidad de acción cuando ocurre un incidente de este tipo. Resulta entonces de primordial importancia contar con un plan de respuesta a los mismos, estableciendo claramente la relación entre (i) las alertas y los incidentes de seguridad, (ii) las características particulares de un incidente de seguridad cuando involucra datos personales y; (iii) las etapas del plan de respuesta a incidentes de seguridad.

Dentro de las recomendaciones para el manejo de incidentes de seguridad de los datos personales, es importante considerar que, antes de iniciar con la descripción del proceso de respuesta a incidentes de seguridad, es necesario abordar y tener en cuenta una serie de conceptos base interrelacionados que son: activo, riesgo, alerta, incidente, vulneración y revelación; derivado de que un activo es todo elemento de valor para una institución involucrada en el tratamiento de datos personales, por ejemplo, la base de datos de empleados, el registro de acceso a un edificio, los equipos de cómputo de una oficina, el correo electrónico o el almacenamiento de información en la nube. Los activos son susceptibles a amenazas, es decir, a factores externos que tienen el potencial de dañarlos, por ejemplo, una descarga eléctrica puede dañar un equipo de cómputo, o un empleado podría acceder a información sin que esté autorizado para ello. Para que una amenaza tenga efecto, requiere explotar una vulnerabilidad, debilidad o falla propia de un activo, por ejemplo, la descarga eléctrica sólo puede afectar a los equipos de cómputo que no tenga un regulador de voltaje. Por otro lado, el empleado podría acceder sin autorización a una base de datos si no está protegida con contraseña.

Para identificar un incidente de seguridad, se requiere de la detección y/o registro de alertas de seguridad, los cuales son advertencias respecto a cambios en los sistemas de tratamiento. Sin embargo, dichas alertas no siempre implican que haya ocurrido un incidente de seguridad. Además, si no se tienen suficientes medidas de seguridad, puede ocurrir un incidente sin que éste se detecte. Cuando se identifica o reporta una alerta de seguridad que involucra información comprometida o daño a los activos, se habla de un incidente de seguridad.

Una vez ocurrido lo anterior, se deberán tomar ciertas medidas entre ellas la de informar de lo ocurrido al titular de los datos personales vulnerados, como lo estipula los artículos 33 y 34 de la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados, y los artículos 37 y 38 de nuestra ley local en la materia. Por tanto, tener en cuenta que, en el sector público estos incidentes consideran:

a) Informar a los titulares de los datos personales lo siguiente:

1. La naturaleza del incidente.
2. Los datos personales afectados.
3. Las recomendaciones al titular acerca de las medidas que éste puede adoptar para protegerse.
4. Las acciones correctivas realizadas de forma inmediata.
5. Los medios donde los titulares pueden obtener más información.
6. La descripción de las circunstancias generales en torno a la vulneración ocurrida, que ayuden al titular a entender el impacto del incidente.
7. Cualquier otra información y documentación que considere conveniente para apoyar a los titulares.

b) Informar a la Autoridad Garante local de la vulneración de seguridad ocurrida.

c) La actualización del documento de seguridad correspondiente.

d) Contar con una bitácora de las vulneraciones en la que se describa:

1. En qué consistió la vulneración.
2. La fecha en la que ocurrió.
3. El motivo o causa de la vulneración.
4. Las acciones correctivas implementadas de forma inmediata y a largo plazo.

e) La imposición de sanciones por la autoridad correspondiente debido a la falta de implementación de medidas de seguridad.

Aunado a lo anterior, existen las denominadas **revelaciones**, las cuales son incidentes de seguridad **que exponen la información a través de Internet o en medios masivos de comunicación**. Las revelaciones de información pueden resultar en una vulneración de seguridad graves al exponer datos personales a un sin número de terceros. Cuando se identifica que una revelación expone datos personales, el responsable debe tomar todas las medidas que estén a su alcance para mitigar la difusión o publicación de los mismos. Por ejemplo, solicitar la baja de contenido al administrador de una página web, así como pedir la eliminación de resultados de un motor de búsqueda, a fin de minimizar el daño a los titulares.

REGISTRO DE INCIDENCIAS

El registro de las acciones que pudieran poner en riesgo la seguridad consistente en la pérdida o destrucción no autorizada, robo, extravío o copia no autorizada, uso, acceso, o tratamiento no autorizado, daño, alteración o modificación de la información no autorizada, en cualquier modalidad de incidencia que pudiera presentarse.

Como primer paso, en modo de preparación, en las recomendaciones para el manejo de incidentes de seguridad de los datos personales, se debe contar con los siguientes formatos, que es la lista de contactos internos y externos a la institución que serán los actores principales que intervendrán ante una alerta, riesgo o incidente de seguridad.

DIRECTORIO DE RESPONSABLES

Titular del Instituto Colimense de las Mujeres

Nombre:	Domicilio:	Datos de Contacto:
Mtra. Erika Judith Torres Guzmán	Complejo Administrativo del Gobierno del Estado, Edificio C, Primer Piso, 3er Anillo Periférico, esquina Libramiento Ejército Mexicano S/N, Colonia El Diezmo, C.P. 28010, Colima, Colima.	direccion.imujerescolima@gmail.com (312) 316-2000

Responsable de Protección de Datos Personales

Nombre:	Domicilio:	Datos de Contacto:
Licda. Janeth Adriana Castro Cisneros	Complejo Administrativo del Gobierno del Estado, Edificio C, Primer Piso, 3er Anillo Periférico, esquina Libramiento Ejército Mexicano S/N, Colonia El Diezmo, C.P. 28010, Colima, Colima.	banavim.colima@gmail.com (312) 316-2000

Responsable Jurídico

Nombre:	Domicilio:	Datos de Contacto:
Licda. Andrea Leticia Silva Castro	Complejo Administrativo del Gobierno del Estado, Edificio C, Primer Piso, 3er Anillo Periférico, esquina Libramiento Ejército Mexicano S/N, Colonia El Diezmo, C.P. 28010, Colima, Colima.	icmcoordinacionjuridica@gmail.com (312) 316-2000

Responsable de Tecnologías de la Información

Nombre:	Domicilio:	Datos de Contacto:
Ing. César Augusto Matus Zavala	Complejo Administrativo del Gobierno del Estado, Edificio C, Primer Piso, 3er Anillo Periférico, esquina Libramiento Ejército Mexicano S/N, Colonia El Diezmo, C.P. 28010, Col.	it.icmujeres@outlook.com (312) 316-2000

Responsable de la Unidad de Transparencia

Nombre:	Domicilio:	Datos de Contacto:
Mtro. Alfonso Emmanuel Parra Valdez	Complejo Administrativo del Gobierno del Estado, Edificio C, Primer Piso, 3er Anillo Periférico, esquina Libramiento Ejército Mexicano S/N, Colonia El Diezmo, C.P. 28010, Colima, Colima.	transparencia.icmujeres@gmail.com (312) 316-2000

Las incidencias se deben documentar mediante una “*bitácora*”, de acuerdo al artículo 36 de la Ley de Datos, dice que el responsable deberá llevar una bitácora de las vulneraciones a la seguridad en la que describa los datos siguientes:

- I.Las acciones correctivas implementadas de forma inmediata y definitiva;
- II.Nombre de la(s) persona(s) responsable o responsables;
- III.Describir en qué consistió la vulneración a la seguridad;
- IV.La fecha en la que ocurrió;
- V.El motivo de ésta;
- VI.Número de vulneración o recurrencia de estas;
- VII.Nombre de la persona encargada cuando la vulneración de seguridad devenga de un tratamiento de datos personales efectuado por el responsable; y
- VIII.Los demás que establezcan las disposiciones jurídicas aplicables.

EJEMPLO DE BITÁCORA DE INCIDENCIAS.

Fecha de registro:			
Área del responsable:			
Nombre de la(s) persona(s) responsable(s) del área:			
VULNERACIÓN A LA SEGURIDAD			
Fecha en la que ocurrió:		Número de vulneraciones o recurrencias:	
Descripción:			
Motivo:			
Acciones correctivas implementadas de forma inmediata y definitiva			
Persona que resolvió la vulneración:			
Soporte físico:	Pueden ser: oficios, documentos, expedientes, estantes o archiveros, tanto los dañados como los recuperados.		
Soporte electrónico:	Puede ser: Los campos, registros, tablas, bases de datos o archivos electrónicos, tanto dañados como recuperados		
AUTORIZACIÓN A LA RECUPERACIÓN DE DATOS			
Nombre de quien autoriza:		Fecha de autorización:	
Quien autoriza la recuperación de los datos			

8.- PROGRAMA GENERAL DE CAPACITACIÓN.

El Instituto Colimense de las Mujeres implementará un programa de capacitación para que las personas servidoras públicas conozcan y apliquen las medidas de seguridad relacionadas con el tratamiento de datos personales. La capacitación se organizará según las funciones y responsabilidades de cada puesto, con atención especial a las áreas que tratan datos personales sensibles o información de mujeres en situación de violencia, así como datos psicológicos, jurídicos, médicos, familiares, socioeconómicos y de niñas, niños y adolescentes.

Este programa forma parte del sistema de gestión de seguridad del Instituto. Se sustenta en la obligación de diseñar capacitación diferenciada según las responsabilidades del personal y en la inclusión del programa general de capacitación dentro del Documento de Seguridad.

Objetivo general

Fortalecer los conocimientos y prácticas del personal del ICM para que trate los datos personales de manera lícita y segura, prevenga accesos o divulgaciones no autorizados y sepa cómo actuar ante una posible vulneración de seguridad.

Objetivos específicos

- Difundir las obligaciones institucionales y las responsabilidades individuales en materia de protección de datos personales.
- Promover el manejo seguro de expedientes físicos y archivos electrónicos.
- Prevenir pérdida, alteración, destrucción, acceso o divulgación no autorizados.
- Capacitar al personal de acuerdo con los datos y sistemas que utiliza en sus funciones.
- Dar a conocer el procedimiento interno para reportar y atender incidentes o vulneraciones.
- Conservar evidencia de las actividades de capacitación y utilizar sus resultados para actualizar el programa.

Personas destinatarias y contenidos

El programa está dirigido a las personas servidoras públicas del Instituto que, por sus funciones, recaban, consultan, registran, organizan, almacenan, utilizan, comunican o resguardan datos personales. También podrá incluir a personas prestadoras de servicios o terceros cuando tengan acceso a información o sistemas del ICM, conforme a las condiciones de su relación con el Instituto.

Nivel	Personas Destinatarias	Contenidos Principales	Frecuencia y Evidencia
General	Todo el personal	Principios y deberes de protección de datos; confidencialidad; uso autorizado de la información; escritorio y pantalla limpios; prevención de correos o enlaces sospechosos; resguardo de expedientes; reporte de incidentes.	Al menos una vez al año y durante la inducción de nuevo ingreso. Evidencia: lista de asistencia y material utilizado.
Específico por función	Personal de Psicología, Trabajo Social, Jurídico, Refugio, Centros LIBRE, BACOLVIM y demás áreas que traten información sensible	Consulta y circulación de expedientes; acceso según funciones; protección de datos de niñas, niños y adolescentes; entrega segura de información; comunicación con otras áreas o instituciones; resguardo y traslado de	Al menos una vez al año y cuando cambien los procedimientos o sistemas de tratamiento. Evidencia: asistencia y evaluación de aprendizaje.

		documentos.	
Técnico y de gestión	Personal de Tecnologías de la Información, Unidad de Transparencia, Administración, Archivo y personas responsables de sistemas o inventarios	Cuentas individuales y permisos; revisión de accesos; registros de actividad; respaldo y recuperación; eliminación segura según el soporte; manejo de servicios de almacenamiento y correo; atención y documentación de incidentes.	Al menos una vez al año y ante cambios relevantes en sistemas o responsabilidades. Evidencia: asistencia, ejercicios y registros técnicos aplicables.

La capacitación de inducción deberá impartirse, de ser posible, antes de otorgar acceso a datos personales o sistemas institucionales. Cuando esto no sea viable, deberá realizarse dentro del primer mes de incorporación y dejarse constancia.

Calendario de capacitación propuesto

Periodo	Actividad	Participantes principales	Evidencia
Octubre–diciembre de 2026	Difusión del programa y sesión general sobre obligaciones, confidencialidad, resguardo de información y reporte de incidentes.	Todo el personal.	Convocatoria, lista de asistencia, materiales y evaluación breve.
Enero–marzo de 2027	Taller sobre manejo de expedientes y datos sensibles en la atención institucional, incluyendo el intercambio seguro de información.	Áreas operativas y de atención; Centros LIBRE; Centros de Atención Integral CAI.	Lista de asistencia, materiales y ejercicios de aplicación.
Abril–junio de 2027	Sesión técnica sobre cuentas, permisos, respaldos, recuperación de información y controles aplicables a correo y almacenamiento institucional.	Tecnologías de la Información, áreas usuarias de sistemas y responsables de gestión documental.	Registro de participantes, temario y resultados de ejercicios.
Julio–septiembre de 2027	Repaso general y ejercicio práctico de reporte y atención de una posible vulneración; revisión de necesidades para el siguiente ciclo.	Personal designado por las áreas y responsables de atención de incidentes.	Registro del ejercicio, áreas participantes, resultados y acciones de mejora.

La Unidad de Transparencia podrá programar sesiones adicionales cuando se incorporen sistemas, cambien los procesos de tratamiento o se identifiquen necesidades derivadas del análisis de riesgos, del monitoreo o de un incidente de seguridad.

Responsables

- La persona titular del ICM aprobará el programa y promoverá la participación

del personal.

- La Unidad de Transparencia, en coordinación con la persona formalmente designada para apoyar la protección de datos personales, coordinará el calendario, los contenidos generales, las convocatorias y el seguimiento.
- El área de Tecnologías de la Información apoyará los contenidos sobre accesos, sistemas, respaldos y seguridad técnica.
- El área Jurídica podrá apoyar en los contenidos relativos a obligaciones, confidencialidad, comunicaciones y transferencias de datos.
- Las personas titulares de las áreas identificarán al personal que requiere capacitación específica y facilitarán su asistencia.
- El personal participante deberá asistir, aplicar las medidas comunicadas y reportar las necesidades de capacitación que identifique.

Evaluación y seguimiento

La Unidad de Transparencia integrará y conservará la evidencia de cada actividad: convocatoria, temario, materiales, listas de asistencia y, cuando corresponda, resultados de evaluaciones o ejercicios. También llevará un registro del personal capacitado y de quienes deban recibir una sesión de recuperación.

Para evaluar el programa, se utilizarán los siguientes indicadores:

- Porcentaje de personas servidoras públicas capacitadas respecto del personal convocado.
- Porcentaje de actividades realizadas respecto de las programadas.
- Resultados de evaluaciones o ejercicios prácticos.
- Necesidades de capacitación detectadas y acciones de seguimiento.

Al cierre de cada ciclo, la Unidad de Transparencia revisará los resultados con las áreas participantes y propondrá las adecuaciones necesarias para el siguiente periodo. El programa también se revisará cuando existan cambios relevantes en los tratamientos, sistemas, riesgos o medidas de seguridad del Instituto.