DOCUMENTO DE SEGURIDAD PARA LA PROTECCIÓN DE DATOS PERSONALES DE LA SECRETARÍA DE BIENESTAR, INCLUSIÓN SOCIAL Y MUJERES DEL GOBIERNO DEL ESTADO DE COLIMA

INTRODUCCIÓN

Tanto a nivel federal como local, es imprescindible que los entes públicos, a su vez sujetos obligados, protejan la información que generan, recopilan, administran y posean. En esa tesitura, los datos personales hacen referencia a la información concerniente a una persona física individualizada o identificable. Por ello, los datos personales deben protegerse mediante un conjunto coherente de procesos y sistemas diseñados, bien administrados por la propia entidad pública que busque establecer, implementar, operar, monitorear y mejorar los procesos y sistemas relativos a la confidencialidad, integridad y disponibilidad de los mismos.

De acuerdo con la Ley General, así como la legislación local de la materia, el documento de seguridad es aquel instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el responsable del Sujeto Obligado, en este caso la Secretaría de Bienestar, Inclusión Social y Mujeres, para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee.

Así mismo, el documento de seguridad debe mantenerse siempre actualizado y ser de observancia obligatoria para todos los servidores públicos de la Secretaría, así como para las personas externas que, debido a la prestación de un servicio, tengan acceso a los sistemas de tratamiento o al sitio donde se ubican los datos personales.

Por tal motivo, a continuación, se encuentra el contenido del documento de seguridad de la Secretaría de Bienestar, Inclusión Social y Mujeres del Gobierno del Estado de Colima. Este instrumento normativo es el resultado de un profundo análisis al interior de nuestra dependencia, en el cual, de manera exhaustiva, se describen las medidas de seguridad administrativas, físicas y técnicas implementadas y por implementar para garantizar la adecuada protección de los sistemas de tratamiento de datos personales que se recaban y custodian al interior de la misma.

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.
Evaluación de impacto en la protección de datos personales	Documento mediante el cual se valoran y determinan los impactos reales respecto de determinado tratamiento de datos personales, a efecto de identificar, prevenir y mitigar posibles riesgos que puedan comprometer el cumplimiento de los principios, deberes, derechos y demás obligaciones.
INAI	Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.
Instituto	Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos del Estado de Colima.
LAN	Una red de área local o LAN (por las siglas en inglés de *Local Area Network*) es una red de computadoras que abarca un área reducida a una casa, un departamento o un edificio.
Ley	Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de 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 los protección, confidencialidad, disponibilidad e integridad de los datos personales.
Medidas de seguridad administrativas	Políticas y procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, la identificación, clasificación y borrado seguro de la información, así como la sensibilización, formación y capacitación del personal en materia de protección de datos personales.
Medidas de seguridad físicas	Conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento.
Medidas de seguridad técnicas	Conjunto de acciones y mecanismos que se valen de la tecnología relacionada con hardware y software para proteger el entorno digital de los datos personales y recursos involucrados en su tratamiento.
N/A	No aplica.
Responsable	Los sujetos obligados señalados en el artículo 1, párrafo 5, de la Ley General que determinarán los fines, medios y alcance y demás cuestiones relacionadas con un tratamiento de datos personales.

Secretaría	Secretaría de Bienestar, Inclusión Social y Mujeres del Gobierno del Estado de Colima.
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.

MEDIDAS DE SEGURIDAD PARA LA PROTECCIÓN DE LOS DATOS PERSONALES, CARACTERÍSTICAS Y FUNDAMENTACIÓN.

Como ya se mencionó en líneas superiores, la legislación define al documento de seguridad como un instrumento en el cual se describen las medidas de seguridad, en sus tres modalidades, para garantizar la confidencialidad, integridad y disponibilidad de los datos personales. La Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados para el Estado de Colma, definen dichas medidas de seguridad en su artículo 4, fracciones XIX, XX, XXI, XXII, mismos que se desglosan a continuación:

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.

De lo anterior, valdría la pena establecer la diferencia entre un soporte físico y un soporte electrónico, debido a que las medidas de seguridad que están estrechamente relacionadas con el tipo de soportes que la Secretaría va a utilizar. Po ello, se hace referencia a las definiciones que se prevén en las Recomendaciones emitidas por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales:

Soportes físicos.	Soportes electrónicos.
Son los medios de almacenamiento tangibles, 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.	Son los medios de almacenamiento 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.

MEDIDAS DE SEGURIDAD PARA LA PROTECCIÓN DE LOS DATOS PERSONALES IMPLEMENTADAS POR LA SECRETARÍA DE BIENESTAR, INCLUSIÓN SOCIAL Y MUJERES.

MEDIDAS DE SEGURIDAD ADMINISTRATIVAS

Tipo de Medida de Seguridad	Mecanismo de Control	Parámetro en que se realiza
	Documentación de la política de seguridad de la información: La política de seguridad de la información debe ser aprobada por el Despacho de la Secretaría,	Los protocolos de capacitación, prevención y acciones en caso de vulneraciones a la seguridad de los datos personales aprobadas por el Despacho de la Secretaría, y

	publicada y comunicada a todos los empleados y terceras partes relevantes.	contenidas en este instrumento concentrador del documento de seguridad, se transmiten a todas las áreas involucradas en el manejo de datos personales, incluidas sus actualizaciones y modificaciones.
Administrativas	Revisión de la Política de seguridad de la información: La política de seguridad de la información debe ser revisada en intervalos planeados o si ocurren cambios significativos, para asegurar su continua aplicabilidad, adecuación y efectividad.	La Política de seguridad de la información es revisada y evaluada en periodos trimestrales.
	Atender las necesidades de seguridad cuando se trata con ciudadanos: Todos los requisitos identificados de seguridad deben atenderse antes de dar acceso a los ciudadanos, a los activos o información de la organización.	La Unidad de Transparencia de la Secretaría, como ventanilla de atención ciudadana, establece los parámetros de ley para asegurar los archivos y/o documentación cuando se solicite consulta directa a los mismos ante una solicitud de información pública.
	Inventario de activos: Todos los activos deben ser claramente identificados y se debe elaborar y mantener un inventario de los activos más importantes.	Se tiene un inventario de datos personales por cada área de la Secretaría involucrada en el manejo y tratamiento de datos personales.

	Roles y responsabilidades: Los roles y responsabilidades de seguridad de los empleados deben estar definidos y documentados en concordancia con la política de seguridad de la información de la organización.	El sistema de gestión para las medidas de seguridad contenido en este documento de seguridad contiene las especificaciones respecto a los roles y responsabilidades del personal involucrado en el tratamiento de datos personales.
	Términos y condiciones de empleo: Como parte de su obligación contractual, los empleados deben acordar y firmar los términos y condiciones de su contrato de empleo, el cual debe indicar su responsabilidad respecto a seguridad de la información.	De conformidad con el artículo 44 de la LPDPPSOEC, en lo concerniente al deber de confidencialidad; todo el personal encargado de la gestión y tratamiento de datos personales al interior del instituto, debe tener en su expediente laboral, una carta compromiso de confidencialidad firmada, como parte de los requisitos de ingreso.
	Concienciación, educación y entrenamiento de seguridad de la información: Todos los empleados de la institución deben recibir concienciación. Asimismo, debe darse entrenamiento de forma periódica en las políticas y procedimientos organizacionales, conforme a la importancia de su función en el trabajo.	La información y el entrenamiento correspondiente al desempeño institucional y la gestión de la seguridad de los datos personales, debe estar contenida en un plan de capacitación en esta materia. La Unidad de Transparencia podrá gestionar dichas capacitaciones con el Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos del Estado de Colima.

	Administración de medios removibles: Deberán documentarse e implementarse procedimientos para la gestión de medios removibles.	Todo componente extraíble de hardware que sea usado para el almacenamiento de información; está sujeto a los Procedimientos de respaldo y recuperación de datos personales, y en su caso a las Técnicas de Supresión y Borrado Seguro de Datos Personales contenidas en este documento de seguridad.
	Deberán establecerse acuerdos para el intercambio de información y aplicaciones entre el instituto y las entidades externas.	Para ello, se estará a lo estipulado en el Título Quinto, Capítulo Único de la LPDPPSOEC.
	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.	Actividades planteadas y descritas en el Sistema de Gestión para las medidas de seguridad incluidas en el documento concentrador de seguridad.
	Registro de usuarios: Deberá existir un procedimiento formal de registro de usuarios para otorgar y revocar el acceso a todos los sistemas y servicios de información.	Procedimiento formal descrito en el Sistema de Gestión para las medidas de seguridad incluidas en el documento concentrador de seguridad.
	Procedimientos de control de cambios: La implementación de	La planificación trimestral para el monitoreo y revisión las medidas de

	los cambios debe ser controlada mediante el uso de procedimientos formales de control de cambios.	seguridad y el sistema de gestión para la protección de los datos personales permite tener un control de cambios y actualizaciones.
	Se deben establecer procedimientos y responsabilidades de la administración para asegurar una adecuada, ordenada y oportuna respuesta a los incidentes de seguridad	Dichos procedimientos y responsabilidades, están plasmados en el plan de respuesta para incidentes de seguridad de la información y los datos personales.
	Verificación del cumplimiento técnico: Se deben verificar constantemente los sistemas de información para el cumplimiento de los estándares de seguridad.	La planificación trimestral para el monitoreo y revisión las medidas de seguridad y el sistema de gestión para la protección de los datos personales permite tener un control de cambios y actualizaciones.
	Distribución de las responsabilidades de seguridad de la información: Todas las responsabilidades de seguridad deben estar claramente definidas.	El establecimiento de roles y responsabilidades del personal y las áreas encargadas del tratamiento de datos personales, se encuentran definidas en el formato de base de datos, dentro del Sistema de Gestión para las medidas de seguridad.
	Retorno de los activos: Todos los empleados deben regresar a la organización todos los activos que tengan en posesión una vez	Lo anterior como parte de las reglas que forman parte de las relaciones de trabajo entre el personal y el Gobierno del Estado de Colima, a través de la

	se termine el trabajo, contrato o acuerdo.	Dirección de Recursos Humanos y la Coordinación Administrativa.

MEDIDAS DE SEGURIDAD FÍSICAS

Tipo de Medida de Seguridad	Mecanismo de Control	Parámetro en que se realiza
Físicas	Control de ingreso a las instalaciones y diferentes áreas ejecutivas y administrativas del instituto.	El ingreso de los empleados se encuentra supeditado al control de asistencia por huella digital, que es un sistema que gestiona la información de horarios de entrada y salida de los empleados; a su vez, cada responsable de área, tiene la responsiva de mantener bajo llave su sitio de trabajo diario al desocuparse del mismo.
	Los derechos de acceso de todos los empleados a la información e instalaciones de procesamiento de información deben ser removidos en cuanto se termine el trabajo, contrato, acuerdo o cuando se requiera hacer un ajuste.	Junto con la entrega recepción del empleado en un área determinada al finalizar su relación laboral con la Secretaría.
	Perímetro de seguridad física: Los perímetros de seguridad (barreras, tales como paredes, tarjetas que controlan entradas o	Las instalaciones de la Secretaría cuentan con diversas puertas con llave y muros que permiten el control del tránsito y los ingresos a las Unidades

	recepciones) deben ser implementados para proteger áreas que contienen información y sistemas de información.	Administrativas mediante protocolos específicos.
	Eliminación y entrega de los medios de almacenamiento: Los medios deberán eliminarse de modo seguro cuando no se les necesite más, usando procedimientos formales.	Una vez que se ha sido exhaustivo con las técnicas de supresión y borrado Seguro, los dispositivos físicos de almacenamiento y respaldos de información, se desechan y destruyen mediante procedimientos seguros.
	Medios físicos de almacenamiento en tránsito: Cualquier medio que contenga información deberá ser protegido contra acceso no autorizado, mal uso o corrupción durante su transporte más allá de los límites de la organización.	Se cuenta con una Jefatura de Tecnologías de la Información, quienes supervisan el transporte de equipos de cómputo o medios de almacenamiento dentro y fuera de la Secretaría.
	Seguridad de los espacios, ventanales y las bardas perimetrales.	Se asegura de que los ventanales de las diferentes áreas sean herméticos para evitar la entrada de polvo y agua de lluvia; a su vez, se da mantenimiento a las paredes perimetrales de cada área, detectando y previniendo humedad y salitre en las mismas.
	Cuidado, mantenimiento y renovación del mobiliario de oficina.	Cajas de archivo, archiveros, escritorios y cajones de aglomerado o MDF, anaqueles de metal, se encuentran estratégicamente acomodados en cada

		sección y área de la Secretaría, para evitar daños por golpes o humedad.
	Protección del equipo: El equipo debe estar situado y protegido para reducir los riesgos de amenazas y peligros ambientales, y oportunidades de acceso no autorizado.	Los espacios del edificio tienen constante mantenimiento de pintura e impermeabilización, los equipos están situados estratégicamente en espacios con alarma y vigilancia interna.
	Seguridad de los equipos en el exterior: La seguridad debe ser aplicada en equipos en el exterior tomando en cuenta los diferentes riesgos de trabajar fuera de las instalaciones de la organización.	Ya sea por reglamento interno, instrucciones o casos excepcionales de emergencia, se podrá sacar equipo o medios de almacenamiento para trabajar desde casa.

MEDIDAS DE SEGURIDAD TÉCNICAS

Tipo de Medida de Seguridad	Mecanismo de Control	Parámetro en que se realiza
	Eliminación o reutilización segura del equipo: Todos los artículos de equipo que contengan medios de almacenamiento deberán revisarse para asegurar la remoción o sobre-escritura apropiada de cualquier información sensible y "software" de autor antes de su eliminación	Todo medio de almacenamiento o equipo de cómputo, después de pasar por el procedimiento administrativo de baja del inventario, se canaliza a la Jefatura de Tecnologías de la Información para análisis y resguardo.

Técnicas (Seguridad de la Red Interna)	Se deberán implementar controles para la detección, prevención y recuperación de la infraestructura en contra de códigos maliciosos. Se deberán implementar procedimientos de concienciación adecuados.	Se estableció una planeación con base en revisiones trimestrales de la calidad y funcionamiento de los antivirus y protecciones con los que cuentan los equipos.
	Controles de red: Las redes deben ser gestionadas y controladas con el fin de ser protegidas de las amenazas, y para mantener la seguridad de los sistemas y aplicaciones que utilizan la red, incluyendo la información en tránsito.	El servidor y red interna es monitoreado permanentemente para detectar posibles amenazas o fallas por causas fortuitas.
	Registro de auditoría: Se deberán producir y almacenar registros de auditoría relacionados a las actividades de los usuarios, las excepciones, y eventos de seguridad. Estos registros deberán ser utilizados en futuras investigaciones y monitoreo de control de accesos.	Se llevan a cabo bitácoras y registros de auditoría trimestrales en relación a los usuarios de los equipos donde se resguarden y gestionen datos personales.
	Administración de privilegios: Deberá restringirse y controlarse la asignación y uso de privilegios.	La administración del control y asignación de privilegios viene definida de raíz desde la identificación y descripción del formato de base de

		datos, mismas que se integran al Sistema de Gestión.
	Uso de contraseñas: Se deberá exigir a los usuarios que sigan buenas prácticas de seguridad en la selección y uso de las contraseñas.	Se cuenta con el listado de privilegios y contraseñas por usuario de equipo de cómputo y se realiza sensibilización del adecuado cuidado y uso de las mismas.
	Equipos desatendidos: Los usuarios deberán asegurar que los equipos atendidos cuenten con protección adecuada.	Los equipos de cómputo cuentan con antivirus especializado y actualizado para prevenir amenazas externas.
	Identificación y autenticación de usuarios: Todos los usuarios deben tener un identificador único (ID de usuario) para su uso personal, y una técnica de autenticación adecuada debe ser elegido para fundamentar la identidad declarada de un usuario.	Cada trabajador de área administrativa, cuenta con un equipo de cómputo a su resguardo, el cual cuenta con ID de usuario por cada usuario, para garantizar la identidad de quien gestiona la información en el equipo.
	Control de vulnerabilidades técnicas: Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se utilizan. Se debe evaluar la exposición de la organización a las mismas y se deben tomar las medidas	Dicho análisis y especificaciones técnicas y de acción, se encuentran contenidos en el plan de respuesta para incidentes de seguridad de la información y los datos personales.

	apropiadas para enfrentar los riesgos asociados.	
	Respaldos de información: Deberán realizarse copias de respaldo de la información y aplicaciones. Se deberán probar los respaldos de acuerdo a una política establecida.	Las áreas competentes para el tratamiento de datos personales en la Secretaría, realizan de manera periódica un respaldo de la información contenida en su equipo de cómputo. Dicho esquema se encuentra regulado en el Sistema de Gestión para la seguridad de los datos personales.

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 los elementos faltantes en el listado de nuestras medidas de seguridad implementadas en el INFOCOL, se debe implementar nuestro Plan de Trabajo, señalando como control la medida de seguridad faltante, y como parámetro, la acción que se realizará para subsanarlo.

MEDIDAS DE SEGURIDAD ADMINISTRATIVAS

CONTROL	PARÁMETRO DE REALIZACIÓN
Documentación de la política de seguridad de la información: La política de seguridad de la información debe ser aprobada por el Despacho de la Secretaría, publicada y	Los instrumentos normativos como el Documento de seguridad, Sistema de Gestión para la protección de los datos personales y el Programa anual de Protección de Datos Personales serán aprobados una vez se

comunicada a todos los empleados y terceras partes relevantes.	concrete la fecha según el calendario final de actividades.
Revisión de la Política de seguridad de la información: La política de seguridad de la información debe ser revisada en intervalos planeados o si ocurren cambios significativos, para asegurar su continua aplicabilidad, adecuación y efectividad.	Se realizará una valoración trimestral de la vigencia y actualidad de la política de seguridad de la información, misma que se traduce en el monitoreo los cambios y la vigencia de los instrumentos normativos desarrollados para la gestión y seguridad de los datos personales.
Términos y condiciones de empleo: Como parte de su obligación contractual, los empleados deben acordar y firmar los términos y condiciones de su contrato de empleo, el cual debe indicar su responsabilidad respecto a seguridad de la información.	Se establecerá como parte del expediente único que la Coordinación Administrativa recaba de cada trabajador al momento de su contratación, la obligatoriedad contractual de comprometerse a resguardar y proteger la información que gestiona, así como también firmar carta de confidencialidad en relación al tratamiento de datos personales ordinarios y sensibles.
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.	Diseñar reportes y bitácoras trimestrales de revisión de la información que se gestiona por cada una de las áreas que dan tratamiento a datos personales, así como los sistemas en que se soportan, para la detección de posibles vulneraciones o riesgos.
Registro de usuarios: Deberá existir un procedimiento formal de registro de usuarios para otorgar y revocar el acceso a todos los sistemas y servicios de información.	Que la totalidad del personal que gestiona información en equipo y soporte electrónico, tenga un usuario y contraseña debidamente registrado.

Distribución de las responsabilidades de seguridad de la información: Todas las responsabilidades de seguridad deben estar claramente definidas.	Junto con el personal que conforma el equipo de atención a incidentes de seguridad de la información, se crearan políticas definidas de intervención y reacción por parte de todo el personal.

MEDIDAS DE SEGURIDAD FÍSICAS

CONTROL	PARÁMETRO DE REALIZACIÓN
Los derechos de acceso de todos los empleados a la información e instalaciones de procesamiento de información deben ser removidos en cuanto se termine el trabajo, contrato, acuerdo o cuando se requiera hacer un ajuste.	Al momento de su contratación, el trabajador adquiere la obligatoriedad contractual de realizar entrega recepción del cargo que finaliza, lo cual implica todo lo relacionado a privilegios otorgados para el manejo de Software y Hardware institucionales.
Seguridad de los espacios, ventanales y las bardas perimetrales.	Se llevan a cabo mantenimientos y renovaciones solo cuando ya es evidente un daño material. Por lo cual se establecerá un diagnóstico semestral por parte del personal de Administración para mantenimiento de los espacios.
Se deberán producir y almacenar registros de auditoría relacionados a las actividades de los usuarios, las excepciones, y eventos de seguridad. Estos registros deberán ser utilizados en futuras investigaciones y monitoreo de control de accesos.	Dadas las características físicas de los equipos de cómputo, archiveros y anaqueles metálicos, que conllevan en si riesgos de deterioro físico; el diagnóstico de mantenimiento, será parte de una auditoría anual a las instalaciones en relación a los bienes muebles mencionados.

La seguridad debe ser aplicada en equipos en el exterior tomando en cuenta los diferentes riesgos de trabajar fuera de las instalaciones de la organización.	Por normatividad interna, no se puede sacar activos ni equipo de las instalaciones; sin embargo, para situaciones emergentes de desarrollará normatividad interna al respecto.

MEDIDAS DE SEGURIDAD TÉCNICAS

CONTROL	PARÁMETRO DE REALIZACIÓN
Se deberán implementar controles para la detección, prevención y recuperación de la infraestructura en contra de códigos maliciosos. Se deberán implementar procedimientos de concienciación adecuados.	Se lleva a cabo de manera periódica la revisión y actualización de los antivirus que protegen los equipos, sin embargo, es necesario fortalecer los procedimientos internos de capacitación y concienciación del personal.
Registro de auditoría: Se deberán producir y almacenar registros de auditoría relacionados a las actividades de los usuarios, las excepciones, y eventos de seguridad. Estos registros deberán ser utilizados en futuras investigaciones y monitoreo de control de accesos.	No se realiza actualmente. Dadas las características del Software y los equipos de cómputo que conllevan en si riesgos de vulneraciones físicas y electrónicas; se realizará una auditoría anual a las actividades de los usuarios, las excepciones, y eventos de seguridad que se hayan suscitado.
Uso de contraseñas: Se deberá exigir a los usuarios que sigan buenas prácticas de seguridad en la selección y uso de las contraseñas.	La Jefatura de Tecnologías de la Información, establecerá dentro de las supervisiones, que el total del personal que maneja equipo de cómputo se suscriba a la práctica de seguridad mediante uso de contraseña.
Todos los usuarios deben tener un identificador único (ID de usuario) para su	En proceso.

uso personal, y una técnica de autenticación adecuada debe ser elegido para fundamentar la identidad declarada de un usuario.

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 por la Secretaría de Bienestar, Inclusión Social y Mujeres, 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 trimestrales y cada área administrativa llevan un control calendarizado.
ELECTRÓNICO	Correos electrónicos	1.- Análisis trimestral 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 de la Secretaría, 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 la dependencia.

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 permita 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.

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 casusas fortuitas.

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 intangibles 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.

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.