GOBIERNO DEL
ESTADO DE COLIMA

INCODIS
Instituto Colimense para la Discapacidad

DOCUMENTO DE SEGURIDAD PARA LA PROTECCIÓN DE LOS DATOS PERSONALES DEL INSTITUTO COLIMENSE PARA LA DISCAPACIDAD

Introducción.

Tanto en la federación, como en toda organización, organismo o entidad de la administración pública del Estado de Colima, se reconoce de manera indubitable, que la información es un activo que, al igual que sus instalaciones, capital humano y recursos financieros, debe 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 la información, aplicando un enfoque basado en los riesgos que se afrontan; llevando a cabo una correcta administración de riesgos a fin de que éstos puedan ser asumidos, mitigados, transferidos o evitados de manera eficiente, sistemática y estructurada, que se adapte a los cambios que se produzcan en el entorno y en la información.

Como sabemos, las vulneraciones de seguridad generan altos costos institucionales además de afectaciones en la esfera de otros derechos y libertades fundamentales de las personas. Es por ello que no resulta conveniente escatimar recursos y esfuerzos en el establecimiento de controles para la protección de la información frente a acciones o situaciones no deseadas, pues de esa manera, además de garantizar la continuidad de la operación de los sujetos obligados, se protege a los individuos a los que se refiere dicha información. Por lo anterior, para efecto de conocer el tipo de controles a que se hace referencia, éstos deben estar documentados, estructurados y ser difundidos para el conocimiento de todos los involucrados en el tratamiento de la información en el Instituto Colimense para la Discapacidad, de conformidad con la Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados para el Estado de Colima.

A este respecto, el CAPÍTULO II “DE LOS DEBERES” de nuestra ley en la materia, define en su artículo 4 fracción XII al Documento de Seguridad, como un 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. Por su parte, en el artículo 38 y 39 de la misma ley, se especifican los elementos que debe contener dicho documento, así como los parámetros y los eventos por los cuales, deberá ser actualizado con cierta periodicidad.

El documento de seguridad es pues, un instrumento normativo en el cual de manera exhaustiva, y derivado de un profundo análisis al interior de nuestra institución pública, 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.

Contenido

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.
INCODIS	Instituto Colimense para la Discapacidad
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	Las persona servidora pública que labora en el INCODIS y tiene relación con el 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.

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 Colma en dichos preceptos normativos, definen dichas medidas de seguridad en su artículo 4, fracciones XIX, XX, XXI, XXII; 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. Para lograr lo anterior, es preciso referirse a las definiciones que se prevén en las Recomendaciones emitidas por el INAI:

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. El Decimoséptimo y el Trigésimo de los Lineamientos hacen mención de los conceptos arriba señalados cuando se alude a los tipos de soportes, medios de almacenamiento o formatos —físicos o electrónicos— en los cuales residen los datos personales del sistema que custodia el sujeto obligado. 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.

Diagnóstico de la institución.

Para identificar claramente el nivel de seguridad en la protección de los datos personales con el que cuenta actualmente el Instituto Colimense para la Discapacidad, es preciso realizar un diagnóstico inicial, el cual se puede esbozar a través de la descripción y

desarrollo del análisis de riesgo y análisis de brecha, mismos que nos permitirán conocer el estado actual que guardan nuestros sistemas de gestión y seguridad en la protección de los datos personales, de los cuales la institución hace tratamiento. Lo anterior, para poder fijar metas y objetivos claros de implementación de controles, medidas de seguridad y estrategias encaminadas a cumplir con dicha finalidad.
En este sentido, se describe a continuación el resultado del análisis de riesgo y el análisis de brecha realizado al interior del Instituto Colimense para la Discapacidad

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 definido de manera más concreta en los Lineamientos Generales de Protección de Datos Personales para el Sector Público; los cuales establecen en su artículo 60 los puntos a considerar para realizar el análisis de riesgo contenido en el Documento de Seguridad; mandatado de igual forma en el artículo 42, 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:

Tipo de Dato	Nivel de Riesgo Inherente	Volumen de Titulares				
		<500k	<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

FACTOR Beneficio: El nivel de riesgo por tipo de dato.

En Proceso de Elaboración Clasificación de los Datos Personales del INCODIS

Análisis de Brecha.

En Proceso de Elaboración

Identificación de las Medidas de seguridad implementadas en el INCODIS

En proceso de elaboración

Medidas de Seguridad ADMINISTRATIVAS
Medidas de Seguridad TÉCNICAS
Medidas de Seguridad FÍSICAS

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 INCODIS, 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 INCODIS, 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 este 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 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.

En el caso de este Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos del Estado de Colima, no se realiza ningún tipo de transferencia de datos personales.

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.

En el caso de este Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos del Estado de Colima, 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 este Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos del Estado de Colima, 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 de este Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos del Estado de Colima, no se realiza ningún tipo de transferencia mediante el traslado en relación a las redes electrónicas.

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

En proceso de elaboración

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, y en concordancia con el acuerdo plenario del INCODIS que así lo establece, se deberá emitir un dictamen de baja y supresión de la información contendida 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 utilizada por el personal de la Secretaría de Informática, para la supresión y borrado seguro de la información que contenga datos personales.

Inventario de datos y sistemas de tratamiento. El inventario de datos personales y de los sistemas de tratamiento de datos personales, es una herramienta primaria en la identificación de aquellos datos que se recaban y gestionan, así como también de los controles mínimos de seguridad para su tratamiento y por su puesto 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 de transparencia, 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.

En proceso de elaboración

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.

El INAI, en su documento de Recomendaciones para el manejo de incidentes de seguridad de los datos personales, menciona 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 organización, involucrado 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 el artículo 40 de la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados, y el artículo 49 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 al Órgano Garante local (INCODIS) 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.
Una vez expuesto lo anterior a manera de introducción y por considerarse relevante y pertinente, se presenta a continuación el Plan de respuesta a incidentes de seguridad de los datos personales del INCODIS, el cual se enfoca, a través de seis etapas, en la mejora continua, a través de estándares internacionales en la materia y de innovaciones tecnológicas.

Plan de contingencia y de respuesta a incidentes de seguridad del INCODIS.

Se consideran 6 etapas, comenzando con la etapa A.- Preparación, continuando con los procesos B, C, D, E, F.

A.- Preparación. A.1 Consideraciones generales.

La fase de preparación consiste en identificar e implantar medidas de seguridad, mientras no se presente un incidente, por ello se recomienda la implementación de un sistema de gestión que permita la mejora continua de la seguridad en una organización; consecuentemente la información contenida en este Plan de respuesta a incidentes de seguridad, será parte también del Sistema de Gestión para la Seguridad de los Datos Personales del INCODIS, que es parte de la triada del deber de seguridad que nos mandata la ley en esta materia, correspondiente a las medidas de seguridad, el sistema de gestión y el documento de seguridad para la protección de los datos personales que tratamos.

Continuando con el punto, como primer paso en este plan de respuesta, se cuenta con un inventario de preparación, a través de una tabla que permite conocer lo siguiente:

a) La relación que existe entre los activos, sus medidas de seguridad, las alertas que se proporcionan a través de dichas medidas, y su propósito, a fin de mitigar un incidente de seguridad.

b) Los activos desprotegidos o carentes de medidas de seguridad para mitigar un incidente.

Así, de manera general y esquematizada podemos visualizar el tipo de alerta que puede darse dependiendo de nuestro activo, y que medida de seguridad pude ayudarnos a mitigarla:

Inventario de Preparación (En proceso de elaboración)

A.2 Respaldos o copias de seguridad.

La creación de respaldos o copias de seguridad es una medida particularmente importante, ya que nos permite a las instituciones recuperar la información dañada, robada o destruida, así como recobrar la operación normal de sus sistemas de tratamiento, en otras palabras, se lleva a cabo lo siguiente:

- La recuperación de archivos o documentos.
- La restauración completa de sistemas de tratamiento.

Para ello, el INCODIS lleva a cabo **Respaldos completos,** consistentes en realizar una copia completa del archivo o medio de almacenamiento de manera mensual, cada día último del mes. Los respaldos se realizan a documentos físicos y electrónicos, sistemas operativos, software y aplicaciones, bases de datos, o datos de usuario. Para la realización de respaldos, se utilizan sistemas automatizados, considerando los siguientes puntos:

1. ***Periodicidad con la que se realizarán los respaldos:*** Cada mes.

2. ***Donde se resguardan:*** Equipo de Cómputo y archiveros de la Unidad Administrativa.
3. ***Cómo se actualizan:*** Se elimina la copia de seguridad anterior una vez respaldando la nueva.
4. ***Cómo se eliminan:*** Mediante procedimientos borrado seguro.

Para los medios de almacenamiento en formato físico, se realiza la digitalización de los documentos y archivos, esto permite realizar su respaldo de seguridad de manera electrónica.

A.3 Elementos para la respuesta a incidentes.

En el caso de las organizaciones o instituciones públicas pequeñas, dado que se requiere en estos casos de conocimientos técnicos muy específicos y especializados para investigar incidentes de seguridad complejos, se recomienda que centren sus esfuerzos en la creación y prueba de copias de seguridad de sus activos críticos, entendiendo estos últimos como aquellos activos de información física o electrónica, que de perderse o de ser vulnerada, evitaría el poder mantener la capacidad de operar con normalidad las actividades y atribuciones de la propia institución.

Por ejemplo, de todos los sistemas de información de una institución, si se vulneran **activos críticos** como las bases que contienen datos personales, se pierde la capacidad de responder a las solicitudes de derechos de acceso, rectificación, cancelación y oposición, que establece la normativa en protección de datos personales. Lo anterior, puede tener consecuencias para el responsable, tales como: apercibimientos, amonestaciones y sanciones.

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.

CONTACTOS INTERNOS:

En proceso

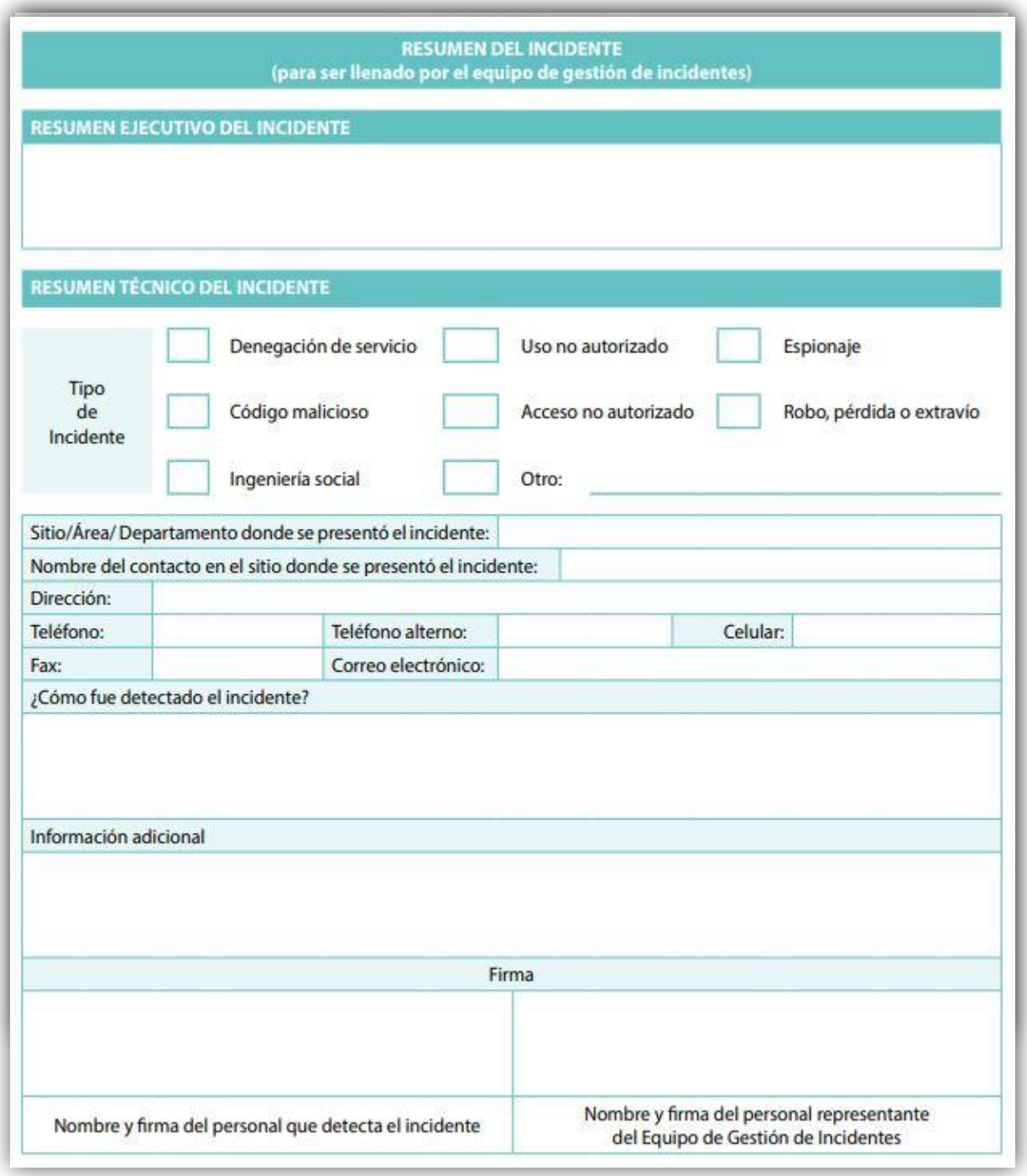
CONTACTOS EXTERNOS:

En proceso

B. Identificación

En esta etapa se detectan las alertas de seguridad y se determina si éstas son incidentes. Se recomienda utilizar un formato específico para documentar una o más alertas que se consideren relevantes o que se relacionen con un incidente de seguridad. Aunado a lo anterior, se recomienda que al menos dos personas estén involucradas en la identificación de un incidente, una para evaluar el incidente e identificar activos que pudieran ser afectados, y otra dedicada a documentar y recabar evidencia. A continuación se muestran los formatos a utilizar:

Hoja 2



RESUMEN DEL INCIDENTE
(para ser llenado por el equipo de gestión de incidentes)

RESUMEN EJECUTIVO DEL INCIDENTE

RESUMEN TÉCNICO DEL INCIDENTE

Tipo de Incidente					
	☐ Denegación de servicio	☐ Uso no autorizado	☐ Espionaje		
	☐ Código malicioso	☐ Acceso no autorizado	☐ Robo, pérdida o extravío		
	☐ Ingeniería social	☐ Otro:			

Sitio/Área/ Departamento donde se presentó el incidente:					
Nombre del contacto en el sitio donde se presentó el incidente:					
Dirección:					
Teléfono:		Teléfono alterno:		Celular:	
Fax:		Correo electrónico:			

¿Cómo fue detectado el incidente?

Información adicional

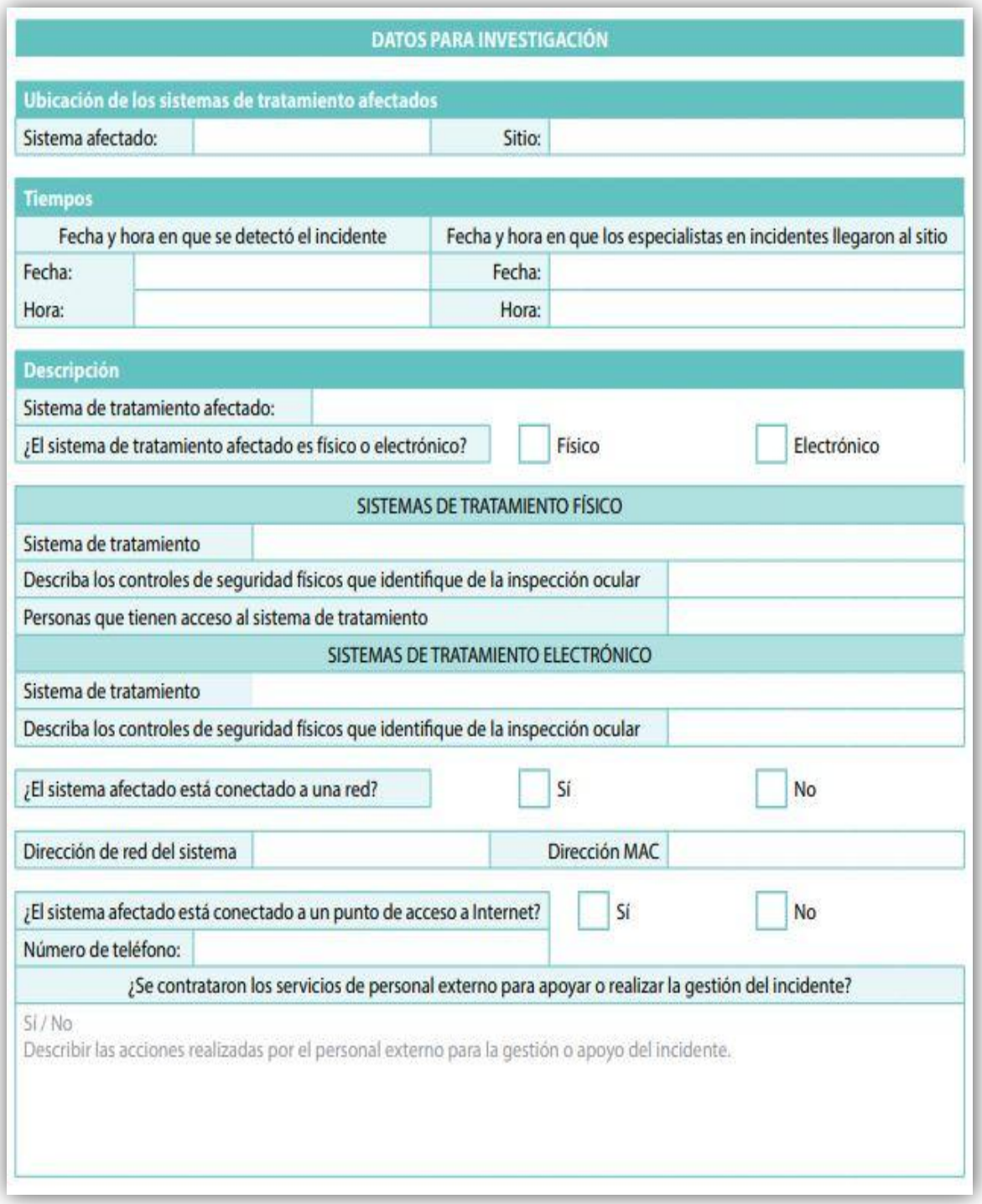
Firma	
Nombre y firma del personal que detecta el incidente	Nombre y firma del personal representante del Equipo de Gestión de Incidentes

C. Contención

Cuando una alerta permite distinguir un incidente de seguridad, se procede a la fase de contención, a fin de limitar el alcance o impacto del incidente identificado. Durante la contención se tienen que aislar los activos afectados. Por ejemplo, si se trata de medios de almacenamiento físico, se aísla el entorno donde ocurrió el incidente como el archivero u oficina. O bien, si se trata de un medio de almacenamiento electrónico, se separan los equipos de cómputo afectados de la red, para evitar, por ejemplo, la propagación de una infección de software malicioso.

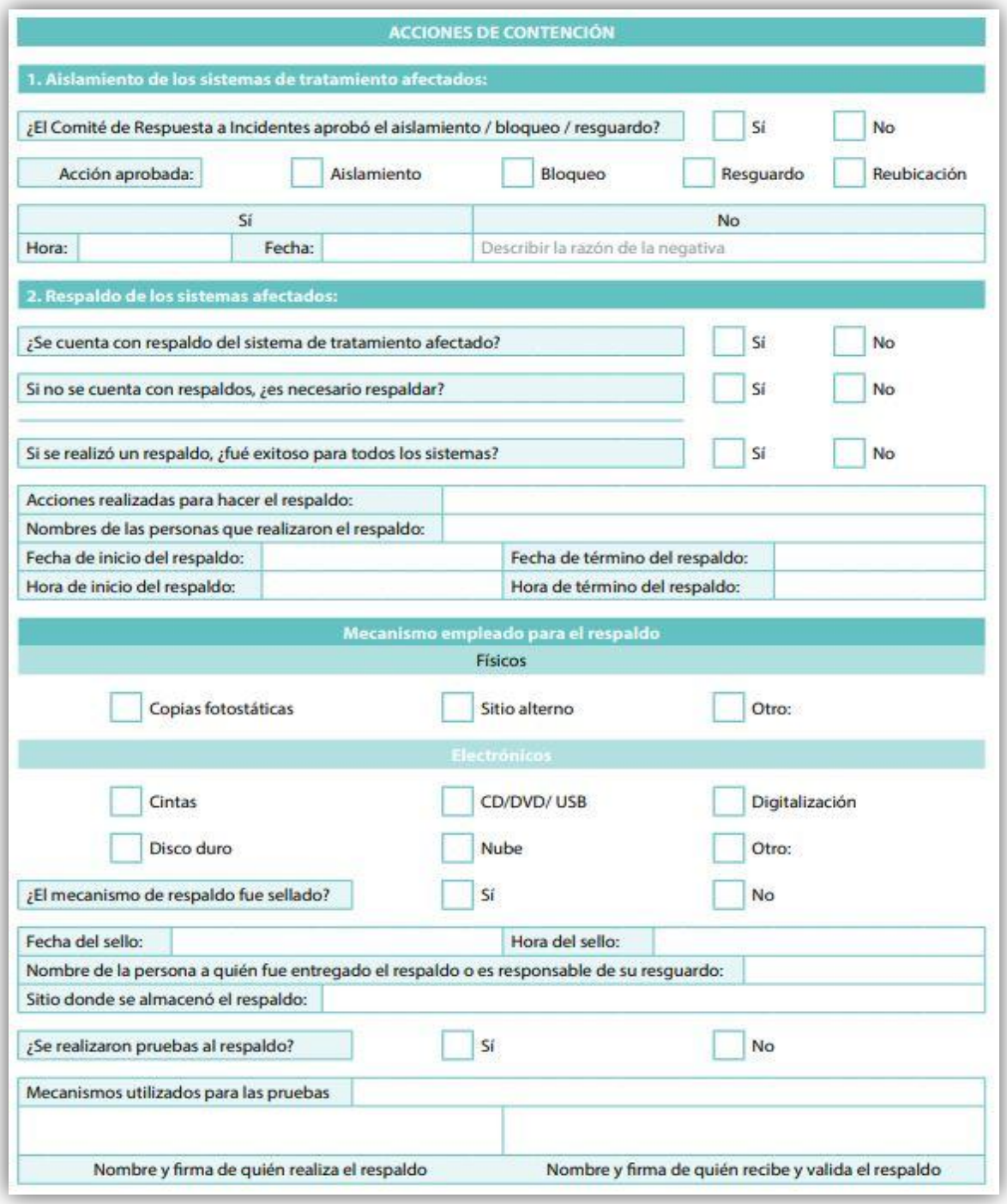
El aislamiento de sistemas y la puesta en operación de respaldos son acciones a corto plazo para reducir los efectos de un incidente. Para proseguir a la contención del incidente a largo plazo se deben identificar las vulnerabilidades explotadas en los activos, así como las medidas de seguridad que pudieron hacer falta, para su posterior implementación. A este respecto, al presentarse un incidente de seguridad, se hace necesario iniciar con la investigación que nos lleve determinar sus causas, para ello nos podemos auxiliar en los siguientes formatos:

Hoja 1



DATOS PARA INVESTIGACIÓN			
Ubicación de los sistemas de tratamiento afectados			
Sistema afectado:		Sitio:	
Tiempos			
Fecha y hora en que se detectó el incidente		Fecha y hora en que los especialistas en incidentes llegaron al sitio	
Fecha:		Fecha:	
Hora:		Hora:	
Descripción			
Sistema de tratamiento afectado:			
¿El sistema de tratamiento afectado es físico o electrónico?	☐ Físico	☐ Electrónico	
SISTEMAS DE TRATAMIENTO FÍSICO			
Sistema de tratamiento			
Describa los controles de seguridad físicos que identifique de la inspección ocular			
Personas que tienen acceso al sistema de tratamiento			
SISTEMAS DE TRATAMIENTO ELECTRÓNICO			
Sistema de tratamiento			
Describa los controles de seguridad físicos que identifique de la inspección ocular			
¿El sistema afectado está conectado a una red?	☐ Sí	☐ No	
Dirección de red del sistema		Dirección MAC	
¿El sistema afectado está conectado a un punto de acceso a Internet?	☐ Sí	☐ No	
Número de teléfono:			
¿Se contrataron los servicios de personal externo para apoyar o realizar la gestión del incidente?			
Sí / No Describir las acciones realizadas por el personal externo para la gestión o apoyo del incidente.			

Hoja 2



ACCIONES DE CONTENCIÓN

1. Aislamiento de los sistemas de tratamiento afectados:

¿El Comité de Respuesta a Incidentes aprobó el aislamiento / bloqueo / resguardo?	☐ Sí	☐ No

Acción aprobada:	☐ Aislamiento	☐ Bloqueo	☐ Resguardo	☐ Reubicación

Sí				No
Hora:		Fecha:		Describir la razón de la negativa

2. Respaldo de los sistemas afectados:

¿Se cuenta con respaldo del sistema de tratamiento afectado?	☐ Sí	☐ No
Si no se cuenta con respaldos, ¿es necesario respaldar?	☐ Sí	☐ No
Si se realizó un respaldo, ¿fué exitoso para todos los sistemas?	☐ Sí	☐ No

Acciones realizadas para hacer el respaldo:			
Nombres de las personas que realizaron el respaldo:			
Fecha de inicio del respaldo:		Fecha de término del respaldo:	
Hora de inicio del respaldo:		Hora de término del respaldo:	

Mecanismo empleado para el respaldo

Físicos

☐ Copias fotostáticas ☐ Sitio alterno ☐ Otro:

Electrónicos

☐ Cintas ☐ CD/DVD/ USB ☐ Digitalización

☐ Disco duro ☐ Nube ☐ Otro:

¿El mecanismo de respaldo fue sellado?	☐ Sí	☐ No

Fecha del sello:		Hora del sello:	
Nombre de la persona a quién fue entregado el respaldo o es responsable de su resguardo:			
Sitio donde se almacenó el respaldo:			

¿Se realizaron pruebas al respaldo?	☐ Sí	☐ No

Mecanismos utilizados para las pruebas	
Nombre y firma de quién realiza el respaldo	Nombre y firma de quién recibe y valida el respaldo

D. Mitigación (Erradicación)

En esta etapa se realiza el tratamiento profundo del incidente de seguridad para minimizar la posibilidad de que éste se vuelva a repetir. La etapa de mitigación considera la creación de un plan de implementación de medidas de seguridad, por ejemplo, para reforzar la seguridad de los medios de almacenamiento físico, se deben mejorar las políticas y los controles de acceso físico, por ejemplo, mejores cerraduras. Para los medios de almacenamiento electrónico, la mitigación incluye actualizaciones de hardware y software, así como revisiones con herramientas automatizadas sobre los respaldos que se pusieron en operación.

El siguiente formato de mitigación, permite registrar los controles y medidas de seguridad a implementar. Se considera también el formato de cadena de custodia, para continuar con la investigación del incidente que se inició en la fase de contención, a fin de arrojar nueva información para la erradicación y para generar evidencia en caso de continuar con un proceso legal, incluso para la creación de documentos de investigación para aquellos interesados en el tema.

Hoja 1

DESCRIPCIÓN DE LAS ACCIONES DE MITIGACIÓN

1. Personal involucrado

Nombre de las personas que realizaron el análisis del sistema de tratamiento afectado:

Iniciales	Nombre completo	Puesto

2. Descripción de las vulnerabilidades detectadas:

¿Fueron identificadas vulnerabilidades? ☐ Sí ☐ No

Tipo de activo[51]	Vulnerabilidad	Descripción	Impacto
			Alto
			Medio
			Bajo

Acciones realizadas para erradicar las vulnerabilidades detectadas

3. Validación:

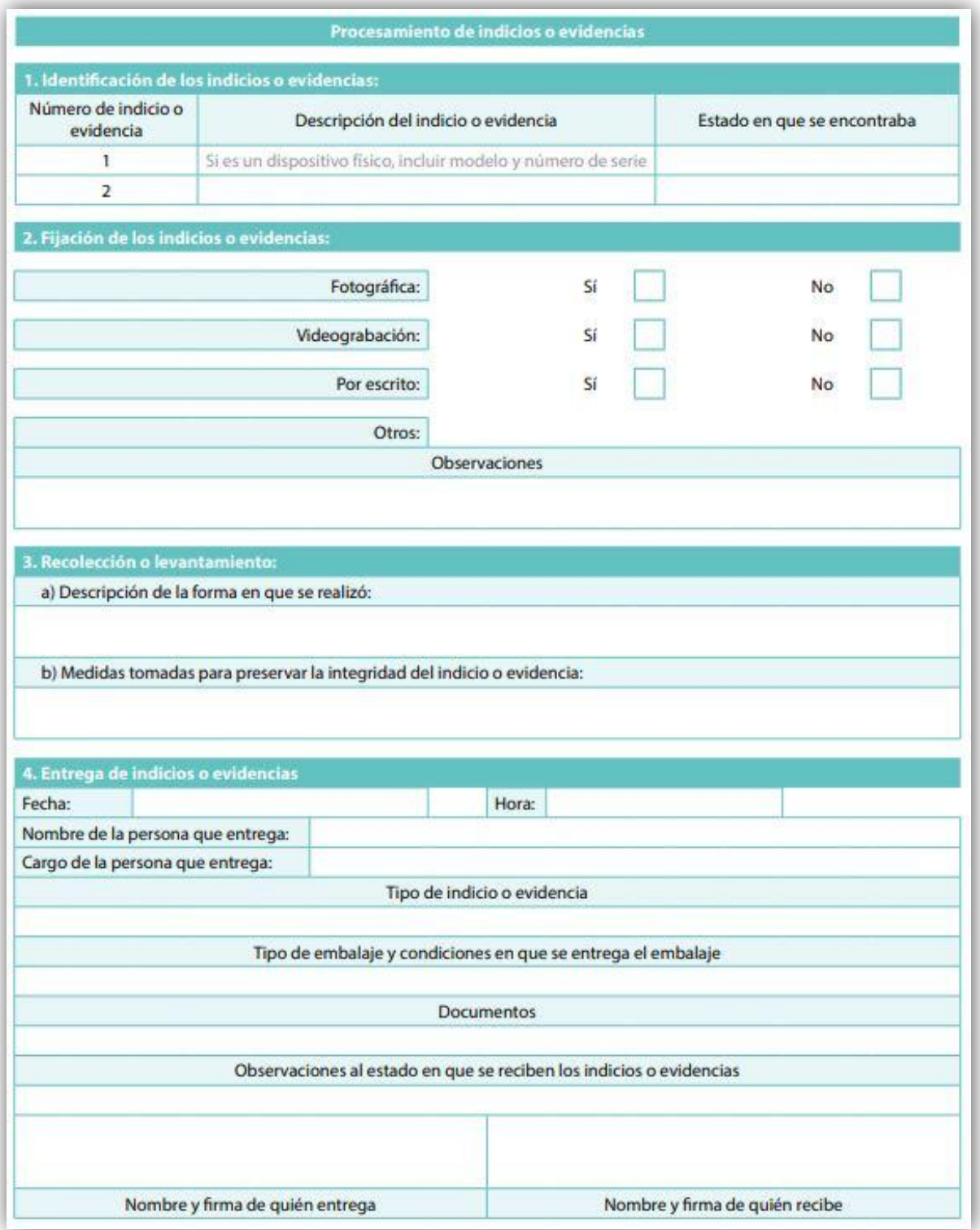
¿Cuál fue el procedimiento de validación usado para asegurar que el problema fue erradicado?

4. Cierre:

Fecha y hora del cierre del incidente:

Nombre y firma de quién realiza la erradicación	Nombre y firma de quién validó la erradicación

Hoja 2



Procesamiento de indicios o evidencias

1. Identificación de los indicios o evidencias:

Número de indicio o evidencia	Descripción del indicio o evidencia	Estado en que se encontraba
1	Si es un dispositivo físico, incluir modelo y número de serie	
2		

2. Fijación de los indicios o evidencias:

Fotográfica:	Sí	☐	No	☐
Videograbación:	Sí	☐	No	☐
Por escrito:	Sí	☐	No	☐
Otros:				

Observaciones

3. Recolección o levantamiento:

a) Descripción de la forma en que se realizó:

b) Medidas tomadas para preservar la integridad del indicio o evidencia:

4. Entrega de indicios o evidencias

Fecha:		Hora:	
Nombre de la persona que entrega:			
Cargo de la persona que entrega:			

Tipo de indicio o evidencia

Tipo de embalaje y condiciones en que se entrega el embalaje

Documentos

Observaciones al estado en que se reciben los indicios o evidencias

Nombre y firma de quién entrega	Nombre y firma de quién recibe

E. Recuperación

Se debe dar seguimiento a las medidas implementadas en la mitigación, y los activos que fueron afectados se reintegran a los sistemas de tratamiento. No todos los activos afectados pueden volver a la operación normal, en este caso se debe documentar el o los activos que entran en sustitución, y el proceso de eliminación de los activos que ya no serán utilizados. Esta fase también contempla el monitoreo de los sistemas de tratamiento a fin de identificar si las nuevas medidas de seguridad no causan algún malfuncionamiento en el sistema, o si éstas funcionan adecuadamente; el monitoreo podría ser temporal, o permanente a través del uso de herramientas automatizadas; por los anterior, se recomienda hacer una simulación del incidente que llevó a la implementación de las nuevas medidas de seguridad, para corroborar que dichos controles pueden evitar que un incidente similar se vuelva a repetir, en caso de falla hay que corregir la implementación. El siguiente formato denominado de recuperación del incidente, permite documentar si los activos afectados por un incidente regresaron o no a la operación de rutina y si se mitigaron los riesgos que causaron el incidente.

DESCRIPCIÓN DE LAS ACCIONES DE RECUPERACIÓN

1. Continuidad en la operación

El sistema de tratamiento continua con su operación después del incidente:	☐ Sí	☐ No
En caso de "No" indicar las causas:		

PERSONAL DESIGNADO PARA DAR SEGUIMIENTO A LA RECUPERACIÓN DEL INCIDENTE		
Iniciales	Nombre completo	Puesto

2. Tiempos:

Fecha en que fue detectado	Fecha en que fue atendido por el equipo de respuesta a incidentes	Fecha en que fue cerrado
Hora en que fue detectado	**Hora en que fue atendido por el equipo de respuesta a incidentes**	**Hora en que fue cerrado**

3. Monitoreo:

Describir las acciones que se realizarán para monitorizar las medidas implementadas:	
Describir las herramientas para el monitoreo de las medidas implementadas (si es el caso):	
Nombre y firma de quién realiza la recuperación	Nombre y firma de quién validó la recuperación

F. Mejora continua (Aprendizaje)

El propósito de esta fase es completar la documentación de lo que se hizo respecto al incidente, y comunicar a las partes interesadas el estado de la seguridad de los activos después del incidente. Se debe generar un archivo histórico o bitácora que permita a los encargados de la respuesta a incidentes contar con una base de conocimiento, que pueda ser utilizada para entrenar a nuevos usuarios, empleados e integrantes del equipo de respuesta a incidentes. Se recomienda que el reporte final sobre un incidente que se ha erradicado no sobrepase las dos semanas para su elaboración, a fin de no perder detalles importantes sobre lo aprendido. El siguiente formato versa sobre la mejora continua como referencia de la estructura del reporte final, así como formatos de comunicación para distribuir el reporte.

Si bien, la documentación generada puede utilizarse con fines de entrenamiento general, el reporte completo o la bitácora de incidentes no debería estar a disposición de cualquier usuario, por ello es importante contar con formatos donde se registre a quién se comunica o comparte el aprendizaje de un incidente de seguridad. Una vez cerrado el incidente, el equipo de respuesta debe regresar a la etapa de preparación, a fin de continuar con la implementación de medidas de seguridad que permitan mejorar la atención y detección de alertas, así como la respuesta cuando se presenten nuevos incidentes de seguridad.

Hoja 1

DOCUMENTACIÓN DEL INCIDENTE	
1. Descripción:	
Área involucrada:	
Sistema de tratamiento afectado:	
Información/ datos personales involucrados en el incidente:	
Resumen Ejecutivo	
Acciones realizadas	
Impacto a la organización / institución	

REGISTROS DE COMUNICACIÓN SOBRE EL INCIDENTE					
Comunicación entre A-B					
Fecha:		Hora:		Método (correo, teléfono, email):	
		Iniciador		Receptor	
Nombre:					
Puesto/Área:					
Organización/Institución a la que pertenece:					
Información de contacto:					
Detalles					

Hoja 2

Comunicación entre B-C					
Fecha:		Hora:		Método (correo, teléfono, email):	
		Iniciador		Receptor	
Nombre:					
Puesto/Área:					
Organización/Institución a la que pertenece:					
Información de contacto:					
Detalles					

Comunicación entre C-D					
Fecha:		Hora:		Método (correo, teléfono, email):	
		Iniciador		Receptor	
Nombre:					
Puesto/Área:					
Organización/Institución a la que pertenece:					
Información de contacto:					
Detalles					

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 los elementos faltantes en el listado de nuestras medidas de seguridad implementadas en el INCODIS, 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 Pleno del Organismo Garante, publicada y comunicada a todos los empleados y terceras partes relevantes.	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 cada primero de abril del ejercicio en curso.
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 Secretaría de Administración 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	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

de monitoreo deben ser revisados con regularidad.	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 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.	El área auditora, 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 uso personal, y una técnica de autenticación adecuada debe ser elegido	Derivado de un reciente cambio de inventario de bienes muebles, hay personal que aún no cuenta con ID de identificación en su equipo de cómputo, lo cual atenderá.

para fundamentar la identidad declarada de un usuario.	

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.

Fuentes Consultadas

Ciberseguridad, I. N. (s.f.). Guía sobre borrado seguro de la información. Recuperado el día 03 de febrero del 2021 en: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ciberseguridad_borrado_seguro_metad.pdf

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. (Junio de 2018). Recomendaciones para el manejo de incidentes de seguridad de datos personales. Recuperado el 12 de febrero del 2021 en: http://inicio.inai.org.mx/DocumentosdeInteres/Recomendaciones_Manejo_IS_DP.pdf

ProtektNet. (s.f.). Recuperado el 12 de febrero del 2021 en: https://protektnet.com/servicios/cumplimiento-normativo/analisis-de-brecha-de-seguridad-de-la-informacion/

Pública, I. F. (19 de 07 de 2009). Guía para la elaboración de un Documento de seguridad v1. Recuperado el 01 de marzo del 2021 en: https://www.ichitaip.org/infoweb/archivos/reader/pdp/Guia_elaboracion_Documento_seguridad.pdf

Instituto de Transparencia, Información Pública y Protección de Datos Personales del Estado de Jalisco. (Agosto del 2018). Guía para la elaboración del Documento de Seguridad. Recuperado el día 18 de marzo del 2021 en: https://www.itei.org.mx/v3/documentos/guias/guia_documento_seguridad_so_31082018.pdf

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. (Junio de 2015). Metodología de Análisis de Riesgo BAA. Recuperado el 04 de marzo del 2021 en:

https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPrivado/Metodolog%C3%ADa_de_An%C3%A1lisis_de_Riesgo_BAA(Junio2015).pdf