SALUD
SECRETARÍA DE SALUD

INSTITUTO NACIONAL DE CARDIOLOGÍA "IGNACIO CHÁVEZ"

INSTITVTO·N·DE CARDIOLOGIA IGNACIO·CHAVEZ

LINEAMIENTOS DE PROTECCIÓN Y SEGURIDAD DE LOS SISTEMAS DE DATOS PERSONALES

AGOSTO, 2007

ÍNDICE

CONTROL DE EMISIÓN			
	Elaboró :	**Revisó :**	**Autorizó**:
Nombre			
Firma			
Fecha			

INSTITUTO NACIONAL DE CARDIOLOGÍA

IGNACIO CHÁVEZ

COMITÉ DE INFORMACIÓN

UNIDAD DE ENLACE

LINEAMIENTOS PARA LA PROTECCIÓN Y SEGURIDAD DE LOS SISTEMAS DE DATOS PERSONALES

Título I

Capítulo 1 Disposiciones Generales

Primero. Los presentes lineamientos tienen por objeto establecer los criterios y medidas de protección y seguridad de los Sistemas de Datos Personales, administrados por el Instituto Nacional de Cardiología Ignacio Chávez, con el propósito de cumplir con lo establecido por los Lineamientos para la Protección de Datos Personales.

Segundo. Los presentes Lineamientos, son aplicables a las áreas que tengan bajo su responsabilidad uno o más Sistemas de Datos Personales, sin contravenir lo dispuesto en la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, su Reglamento y los Lineamientos de Protección de Datos Personales, las Recomendaciones sobre Medidas de Seguridad Aplicables a los Sistemas de Datos Personales emitidas por el IFAI, e incluyen el documento de seguridad a que se refiere el numeral trigésimo tercero de dichos Lineamientos.

Tercero. Todos los archivos que contengan datos personales serán información confidencial y su administración y resguardo estarán a cargo del Responsable del Sistema de Datos Personales o de aquel funcionario público, quien en cumplimiento de sus responsabilidades, los hubiera integrado, recibido, obtenido o transformado.

Cuarto. En los presentes lineamientos se emplearán las siguientes definiciones adicionales a las contenidas en los artículos 3 de la LFTAIPG, 2 de su Reglamento, 3 de

los Lineamientos de Protección de Datos Personales y el numeral IV de las Recomendaciones sobre Medidas de Seguridad Aplicables a los Sistemas de Datos Personales:

- **Archivo clínico:** Área del Instituto donde personal especializado organiza y resguarda los expedientes clínicos de los usuarios que acuden a recibir la prestación de algún servicio, realización de estudios o participen en proyectos de investigación.

- **Áreas de Enseñanza:** A las áreas cuyas responsables de las actividades académicas del Instituto Nacional de Cardiología Ignacio Chávez.

- **Área de Tecnologías de la Información:** Al área administrativa responsable del Desarrollo Tecnológico del INCAR.

- **Áreas de Investigación:** A las áreas responsables de la investigación científica del INCAR.

- **Área de Personal:** A las áreas administrativas encargadas del manejo de los expedientes del personal que mantuvo o tiene una relación laboral con el INCAR, en cualquier modalidad de contratación.

- **Área de servicios escolares:** Al área especializada y responsable del registro y control de los datos de las personas (alumnos o participantes) que asistan formalmente a las actividades académicas del INCAR.

- **Archivo de Concentración:** Unidad responsable de la administración de documentos cuya consulta es esporádica por parte de las unidades administrativas de las dependencias y entidades, y que permanecen en él hasta su destino final.

- **Archivo Histórico:** Unidad responsable de organizar, conservar, administrar, describir y divulgar la memoria documental institucional.

- **Archivo de Trámite:** Unidad responsable de la administración de documentos de uso cotidiano y necesario para el ejercicio de las atribuciones de una unidad administrativa.

- **Bioestadística:** Es la aplicación de la estadística a la medicina.

- **Clasificación:** Proceso para determinar y ordenar el tipo de la información que está contenida en los documentos, expedientes y archivos del Instituto. De acuerdo a las características de la información ésta se clasificará en reservada o confidencial con apego a la Ley.

- **Comité:** Al Comité de Información del INCAR, establecido con fundamento en los artículos 29 de la LFTAIPG y 57 de su Reglamento.

- **Comisiones:** Comisiones de Investigación, Ética y Bioseguridad contempladas por el Reglamento de la Ley General de Salud en Materia de Investigación para la Salud.

- **Consentimiento**: Permiso específico, informado y expreso que una persona da libremente para que sus datos genéticos sean recolectados, tratados, utilizados y conservados.

- **Consentimiento informado:** Acuerdo por escrito, mediante el cual el sujeto de investigación o, en su caso, su representante legal autoriza su participación en la investigación, con pleno conocimiento de la naturaleza de los procedimientos y riesgos a los que someterá, con la capacidad de libre elección y sin coacción alguna.

- **Coordinación:** A la Coordinación de Archivos del INCAR, establecida con fundamento en los Lineamientos Generales para la Organización y Conservación de Archivos de las Dependencias y Entidades de la Administración Pública Federal.

- **Datos asociados con una persona identificable:** datos que contienen información como el nombre, la fecha de nacimiento y la dirección, gracias a la cual es posible identificar a la persona a la que se refieren.

- **Datos personales:** información concerniente a una persona física, identificable, relativa a sus orígenes étnico o racial, características físicas, morales o emocionales, a su vida afectiva y familiar, domicilio, teléfono, creencias, preferencias sexuales.

- **Desclasificación de información:** Proceso para determinar que la información deja de tener el carácter de clasificada.

- **Documentos base de la organización de archivos o instrumentos de archivos:** Al conjunto de documentos básicos de organización de los archivos del INCAR conformado por el Cuadro General de Clasificación Archivística, el Catálogo de Disposición Documental y la Guía Simple de Archivos del INCAR aprobados por el Comité de Información y autorizados por la Junta de Gobierno del Instituto.

- **Documento de seguridad:** Documento que contiene las medidas de seguridad administrativas, físicas y técnicas de seguridad aplicables a los sistemas de datos personales.

- **Expediente clínico:** Conjunto de documentos escritos, gráficos e imagenológicos o de cualquier otra índole, en los cuales el personal de salud, deberá hacer los registros, anotaciones y certificaciones correspondientes a su intervención, con arreglo a las disposiciones sanitarias, que sirven como apoyo al personal médico y científico del INCAR en sus labores de investigación, prestación de servicios y/o enseñanza.

- **Fundamento:** Argumento en el que se señala el o los ordenamientos jurídicos (artículo, fracción, inciso y párrafo) que expresamente otorgan el carácter de clasificada a una información.

- **IFAI:** Instituto Federal de Acceso a la Información Pública Gubernamental.

- **INCAR o el Instituto:** Instituto Nacional de Cardiología Ignacio Chávez.

- **Investigación:** Proceso sistemático, organizado y objetivo, cuyo propósito es responder a una pregunta o hipótesis y así aumentar el conocimiento y la información sobre algo desconocido.

- **Investigador:** Persona que se encarga de realizar investigaciones científicas-técnicas.

- **Ley o LFTAIPG:** Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.

- **Lineamientos:** A los Lineamientos para la Protección y Seguridad de los Sistemas de Datos Personales del Instituto Nacional de Cardiología Ignacio Chávez.

- **Lineamientos del IFAI:** A los Lineamientos para la Protección de Datos Personales emitidos por el Instituto Federal de Acceso a la Información Pública Gubernamental publicados en el D.O.F. el 30 de septiembre de 2006.

- **Medidas de seguridad (MS):** Los ordenamientos o políticas establecidas para resguardar los sistemas de datos personales en el INCAR.

- **Patronato:** Al órgano de consulta del INCAR formado por particulares, aprobado por la Junta de Gobierno del Instituto, de acuerdo a la Ley de los Institutos Nacionales de Salud.

- **Principios de Protección de Datos Personales:** Licitud, Calidad de los datos, Acceso y Corrección, De Información, Seguridad, Custodia y Cuidado de la Información y Consentimiento para la Transmisión.

CONTROL DE EMISIÓN			
	Elaboró :	**Revisó :**	**Autorizó**:
Nombre			
Firma			
Fecha			

- **Propiedad Intelectual:** Es el conjunto de derechos patrimoniales de carácter exclusivo que otorga el Estado por un tiempo determinado, a las personas físicas o morales que llevan a cabo la realización de creaciones artísticas o que realizan invenciones o innovaciones y de quienes adoptan indicaciones comerciales, pudiendo ser éstos, productos y creaciones objetos de comercio.

- **Protocolo o Proyecto de Investigación:** Documento que presenta un plan realizado por un científico (investigador) que contiene la información necesaria para la realización de una investigación, es decir, proporciona los antecedentes, las razones y los objetivos, y describe su diseño, metodología y organización, incluyendo consideraciones estadísticas, éticas y de bioseguridad. Algunas de estas consideraciones pueden ser proporcionadas en otros documentos a los que haga referencia el protocolo.

- **Registros de usuarios o participantes:** Se refiere a los registros (temporales o permanentes) que contengan datos personales que se integren con un fin específico como usuarios de la página, asistentes a congresos y eventos académicos y otros registros de personas físicas especiales.

- **Recomendaciones:** a las Recomendaciones sobre Medidas de Seguridad Aplicables a los Sistemas de Datos Personales emitidas por el IFAI publicadas en diciembre de 2006.

- **Sistema de datos personales y/o Sistemas de Datos Personales (SDP o SDP's):** Conjunto (s) ordenado (s) de datos personales que están en posesión de un área administrativa del INCAR.

- **Sistema de datos personales físicos:** Registros manuales, impresos, sonoros y/o magnéticos.

- **Sistema de datos personales automatizados:** Que han recibido un tratamiento informático y requieren herramienta tecnológica específica para su acceso.

- **Titular de los datos:** Persona física a quien se refiere los datos personales que serán objeto de tratamiento.

- **Unidad:** Son las Direcciones, subdirecciones y departamentos hasta nivel de los Laboratorios, Unidades de Alta Tecnología y otras Unidades Especiales del Instituto, en su caso.

- **Versión pública:** Es la versión que se hace de un documento en el que se haya clasificado como reservado o confidencial una (s) sección (es) en el cual el área responsable omite dichas secciones de su contenido, a fin de entregar la información pública. Éstas deben seguir Lineamientos para la elaboración de versiones públicas, por parte de las dependencias y entidades de la Administración Pública Federal publicados en el D.O.F. el 13 de abril de 2006.

Quinto. Los protocolos de investigación, convenios de colaboración o contratos en los cuales se integre un sistema de datos personales se deberá contar con la autorización del Director General.

Sexto. La Unidad de Enlace a través del sistema informático administrado por el IFAI, denominado Sistema “Persona”, reportará las actualizaciones y transmisiones totales o parciales de los Sistemas de Datos Personales administrados por el INCAR.

A) Capítulo Único Los responsables de los sistemas de datos personales

Séptimo. Las áreas del INCAR que administren, generen, obtengan, adquieran, transformen o conserven un sistema de datos personales, deberán nombrar un responsable. Este responsable deberá incorporar los datos referentes al sistema en la aplicación informática establecida por el IFAI para este propósito.

Octavo. Los protocolos de investigación que requieran de contar con sistemas de datos personales, designarán un responsable del mismo dentro del protocolo e informarán a la Unidad de Enlace.

Noveno. Los responsables de los sistemas de datos personales detallarán específicamente el tratamiento, las medidas de seguridad, necesidades de transmisión además de incluir la leyenda de protección y la autorización explicita en los formatos de recolección y en el consentimiento informado.

Décimo. El (los) responsable (s) de los Sistemas de Datos Personales detallarán el tiempo de almacenamiento y la forma de destrucción de acuerdo con el catálogo de disposición documental

B) Capítulo Único La identificación de los sistemas y del nivel de seguridad aplicable

Décimo primero. A fin de determinar si la información que poseen las áreas del Instituto es un dato personal, se deben agotar las siguientes condiciones:

- Que corresponda a una persona física, identificada e identificable.
- Que se encuentre contenida en los archivos o documentos del INCAR.

Décimo segundo. Los sistemas de datos personales podrán ser físicos y/o automatizados:

a) Físicos: Conjunto ordenado de datos que para su tratamiento están contenidos en registros manuales, impresos, sonoros, magnéticos, visuales u holográficos.

b) b) Automatizados: Conjunto ordenado de datos que para su tratamiento han sido o están sujetos a un tratamiento informático y que por ende requieren de una herramienta tecnológica específica para su acceso, recuperación o tratamiento.

Décimo tercero. A todos los sistemas de datos personales administrador por el INCAR deberán aplicarles invariablemente las medidas de seguridad correspondientes al nivel básico establecido en la Recomendaciones emitidas por el IFAI, de acuerdo a las posibilidades y recursos disponibles.

Décimo cuarto. Las medidas de seguridad correspondientes a los niveles medio y alto establecidas en las Recomendaciones, se aplicarán en los casos que proceda y en la medida de las posibilidades de las áreas los recursos disponibles por el INCAR para estos efectos.

Décimo quinto. Los Responsables del Sistema de Datos Personales la Subdirección de Informática o de la Unidad de Enlace en caso necesario, determinarán el nivel de seguridad aplicable a cada sistema de datos personales, basado en el análisis de su contenido, de acuerdo con la siguiente tabla:

Las medidas de seguridad aplicables a todos los sistemas de datos personales.

1. **De Identificación:** Nombre, domicilio, teléfono particular, teléfono celular, correo electrónico, estado civil, firma, firma electrónica, RFC, CURP, cartilla militar, lugar de nacimiento, fecha de nacimiento, nacionalidad, edad, nombres de familiares dependientes y beneficiarios, fotografía, costumbres, idioma o lengua, entre otros.
2. **Laborales:** Documentos de reclutamiento y selección, de nombramiento, de incidencia, de capacitación, puesto, domicilio de trabajo, correo electrónico institucional, teléfono institucional, actividades extracurriculares, referencias laborales, referencias personales, entre otros.

Nivel medio: Medidas adicionales a las de nivel básico.

1. **Datos Patrimoniales**: Bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos y egresos, cuentas bancarias, seguros, afores, fianzas, servicios contratados, referencias personales, entre otros.
2. **Datos sobre procedimientos administrativos seguidos en forma de juicio y/o jurisdiccionales:** Información relativa a una persona que se encuentre sujeta a un procedimiento administrativo seguido en forma de juicio o jurisdiccional en materia laboral, civil, penal o administrativa.
3. **Datos Académicos:** Trayectoria educativa, títulos, cédula profesional, certificados y reconocimientos, entre otros.
4. **Tránsito y movimientos migratorios:** Información relativa al transito de las personas dentro y fuera del país e información migratoria de las personas, entre otros.

Nivel alto: Medidas adicionales a las de nivel básico y medio.

1. **Datos Ideológicos:** Creencia religiosa, ideología, afiliación política y/o sindical, pertenencia a organizaciones de la sociedad civil y/o asociaciones religiosas, entre otros.
2. **Datos de Salud:** Estado de salud, historial clínico, alergias, enfermedades, información relacionada con cuestiones de carácter psicológico y/o psiquiátrico, incapacidades médicas, intervenciones quirúrgicas, vacunas, consumo de sustancias tóxicas, uso de aparatos oftalmológicos, ortopédicos, auditivos, prótesis, entre otros.
3. **Características personales:** Tipo de sangre, ADN, huella digital, u otros análogos.
4. **Características físicas:** Color de piel, color de iris, color de cabello, señas particulares, estatura, peso, complexión, discapacidades, entre otros
5. **Vida sexual:** Preferencia sexual, hábitos sexuales, entre otros.
6. **Origen:** Étnico y racial.

C) Del manejo y protección de los sistemas de datos personales

1 La aplicación de los principios rectores de la protección de datos personales

Décimo sexto. Los Responsables de los Sistemas de Datos Personales aplicarán estrictamente los principios rectores de protección de datos personales. Asimismo el tratamiento de datos personales se hará invariablemente con base en los principios de licitud, calidad, acceso y corrección, de información, seguridad, custodia y consentimiento para su transmisión, de acuerdo con los Lineamientos emitidos para este efecto.

Décimo séptimo. La creación, integración o posesión de SDP obedecerá exclusivamente a las atribuciones legales, reglamentarias y/o las establecidas por la Ley de los Institutos Nacionales de Salud y/o en el Estatuto Orgánico y se obtendrán a través de los medios previstos en la Ley Federal de Transparencia y acceso a la Información Pública Gubernamental y los lineamientos para la protección de datos personales.

Décimo octavo. Los datos personales deberán tratarse únicamente para la finalidad determinada y legítima para la cual fueron obtenidos, sin menoscabo de que, de ser posible ampliar las aplicaciones o tratamiento de los mismos con fines de investigación, estadístico, u otro legalmente aceptado, podrán realizarse, siempre y cuando exista la autorización expresa y ésta quede asentada en el instrumento de recolección, consentimiento informado autorizado entregado al titular de los datos.

Décimo noveno. Los sistemas de datos personales se almacenarán de forma tal que permitan a los titulares de los mismos, el ejercicio de los derechos de acceso y corrección previstos por la Ley, el Reglamento y los Lineamientos emitidos por el Instituto no procediendo en el caso de expedientes clínicos, particularmente en los obtenidos a través de contratos o convenios y/o correspondan a un protocolo de investigación.

En las áreas del INCAR, al momento en que se recaben datos personales, tanto en formatos físicos con en los electrónicos el encargado de este proceso hará del conocimiento al titular, lo siguiente:

a) La protección de los datos conforme a lo dispuesto por la Ley.
b) El fundamento legal para ello.
c) La finalidad del Sistema de datos personales.
d) Periodo de conservación determinado para el biobanco, en su caso.

Vigésimo. Las áreas del INCAR que administren SDP deberán hacer del conocimiento del titular de los datos, al momento de recabarlos, el fundamento y motivo de ello, así como los propósitos para los cuales se tratarán dichos datos a través del documento que contenga la siguiente leyenda:

"Los datos personales serán protegidos, incorporados y tratados en el sistema de datos personales denominado _____, a través _____, así como en _____, lo anterior con fundamento en_____, Ley de los Institutos Nacionales de Salud, NOM-003-SSA2-1993, Reglamento Interior de la Secretaría de Salud, Manual de Procedimientos del Banco de Sangre. Este Sistema de datos Personales fue registrado en el Sistema Persona ante el Instituto Federal de Acceso a la Información Pública, IFAI (www.ifai.org.mx), y podrán ser transmitidos de manera interna a la Dirección General de la Institución, Dirección Médica, Dirección de Enfermería, Departamento de Asuntos Jurídicos, Órgano Interno de Control y Unidad de Enlace, mediante solicitud escrita; así como a algunas otras áreas que requieran información con la finalidad de atender los requerimientos en materia de Atención Médica para contribuir al cumplimiento de los objetivos y metas institucionales, además de otras transmisiones previstas en la Ley. La unidad administrativa responsable del sistema de datos personales es el Banco de Sangre, el interesado podrá ejercer los derechos de acceso y corrección de sus datos personales en la Unidad de Enlace del Instituto Nacional de Cardiología Ignacio Chávez, ubicada en Juan Badiano No. 1, Col. Sección XVI, Delegación Tlalpan.

Lo anterior se informa en cumplimiento del Decimoséptimo de los Lineamientos de Protección de Datos Personales, publicados en el Diario Oficial de la Federación del 30 de septiembre de 2005.

Vigésimo primero: Lo anterior sin prejuicio de que las áreas elaboran sus propios formatos, agregando los elementos que consideren necesarios.

Vigésimo segundo. Los RSDP deberán adoptar las medidas necesarias para garantizar la integridad, confiabilidad, confidencialidad y disponibilidad de los mismos mediante acciones que eviten su alteración, pérdida, transmisión y acceso no autorizado.

Vigésimo tercero. La custodia y cuidado de los datos personales serán responsabilidad directa de los RSDP de las áreas del INCAR, los responsables, encargados, investigadores y usuarios en lo que corresponde al manejo cuidadoso en su tratamiento.

Vigésimo cuarto. Toda transmisión de datos personales deberá contar con el consentimiento explícito del titular de los datos, mismo que deberá otorgarse en forma libre, expresa e informada.

CONTROL DE EMISIÓN			
	Elaboró :	**Revisó :**	**Autorizó**:
Nombre			
Firma			
Fecha			

Capítulo 2

Del tratamiento de los datos personales

Vigésimo quinto. El tratamiento que se dé a los datos personales generados o en posesión de las áreas del INCAR debe cumplir con el principio de calidad y ser exacto, adecuado, pertinente y no excesivo por lo que, en lo posible los sistemas se mantendrán actualizados de manera tal que no altere la veracidad de la información; se observen las medidas de seguridad aplicables; el tratamiento sea realizado por el personal autorizado y la información solicitada sea la estrictamente necesaria para cumplir con los fines para los cuales se recabe.

Vigésimo sexto. En caso de que los titulares de las áreas, RSDP o usuarios detecten que hay datos personales inexactos, se deberán tomar las acciones necesarias para realizar la corrección (de oficio) y actualizarlos en el momento en que tengan conocimiento de la inexactitud de los mismos. No se realizará corrección alguna de datos personales si no se cuenta con los documentos soporte que justifiquen la actualización. En caso de detectar algún dato inexacto o incorrecto y no poseer el documento soporte, deberán implementarse las medidas que permitan la localización del titular de los datos para recabar el soporte documental pertinente.

Vigésimo séptimo. Los titulares de las áreas o los RSDP podrán dar de baja documentos que contengan datos personales que haya prescrito sus valores primario y secundarios observando en el instructivo para las bajas documentales.

Vigésimo octavo Los datos personales sólo podrán ser tratados en sistemas que reúnan las condiciones de seguridad establecidas en los presentes Lineamientos, los Lineamientos del IFAI, las Recomendaciones y las demás disposiciones aplicables.

Vigésimo noveno. Los protocolos de investigación que incluyan la elaboración, posesión e intercambio de sistemas de datos personales, incluirán en el formato de recopilación de información y en el consentimiento informado, la leyenda a que hace referencia el numeral decimoctavo de los Lineamientos del IFAI.

Trigésimo. Las áreas del INCAR que recaben datos personales a través de un servicio de orientación telefónica, página web, formatos de inscripción o de uso en eventos académicos o laborales u otros medios o sistemas, deberán establecer un mecanismo por el que se informe previamente a los particulares que sus datos personales serán recabados, la finalidad de dicho acto así como el tratamiento al cual serán sometidos.

Trigésimo primero. Si se almacenara la información recabada, ésta deberá ser reportada como sistema de datos personales y, dependiendo del tipo de dato, estará sujeta a las medidas de seguridad y garantías aplicables.

Trigésimo segundo. Las áreas administrativas, responsables, encargados, los investigadores y funcionarios del INCAR aplicarán el proceso de disociación, por el cual los datos personales no pueden asociarse al titular de éstos, ni permitir por su estructura, contenido o grado de desagregación, la identificación individual del mismo en todos los casos en los que esto sea posible, particularmente cuando dichos datos requieran de ser compartidos.

Trigésimo tercero. En todos los casos, el tratamiento de datos personales para fines estadísticos deberá efectuarse mediante la disociación de los datos, de conformidad con la Ley de Información Estadística y Geográfica, así como las demás disposiciones aplicables en la materia.

Trigésimo cuarto. Cuando el INCAR contrate o requiera de la participación de un tercero (s) para que realice (n) el tratamiento de datos personales, deberá estipularse en el

contrato o convenio respectivo, la obligatoriedad de conservar la confidencialidad de los mismos, la implementación de medidas de seguridad y custodia previstas en los presentes Lineamientos y los emitidos del IFAI así como, en la normatividad aplicable, así como la imposición de penas convencionales por su incumplimiento.

Capítulo 3

La transmisión con consentimiento del titular

Trigésimo cuarto. La transmisión de sistemas con datos personales generados o en posesión del INCAR sin disociación, sólo se hará cuando:

a) Así lo prevea de manera expresa una disposición legal.
b) Medie el consentimiento expreso de los titulares.

Trigésimo quinto. No podrán transmitirse datos personales si no se cuenta con el consentimiento del titular de los mismos otorgado por escrito incluyendo la firma autógrafa y la copia de identificación oficial con excepción de los casos citados en el siguiente numeral.

Trigésimo sexto. Podrán transmitirse los datos personales sin el consentimiento explícito de los titulares en los siguientes casos:

a) Por razones estadísticas, científicas o de interés general, posterior a la disociación de los mismos.
b) Cuando se transmitan con otras dependencias o entidades, siempre y cuando se utilicen para el ejercicio de atribuciones o facultades.
c) Cuando exista un orden judicial.
d) Cuando se contrate a terceros para la prestación de un servicio. En este caso de suscribirá preferentemente un convenio de confidencialidad.
e) Cuando se requieran para dar cumplimiento al artículo séptimo de la Ley.
f) Cuando sea información de personas a las que se les entreguen por cualquier motivo recursos públicos.

g) Cuando se hubiera recabado o forme parte de un registro o fuente de acceso público.

Trigésimo séptimo. Las transmisiones totales o parciales de sistemas de datos personales que realicen las áreas administrativas e investigadores del INCAR en el ejercicio de sus atribuciones o en el proceso de realización de una investigación, deberán ser notificadas por el responsable del área o por el investigador al IFAI a través del Sistema "Persona" los diez primeros días hábiles de los meses de marzo y septiembre, informando a la Unidad de Enlace.

Trigésimo octavo. El informe deberá contener al menos, lo siguiente:

1. Identificación del Sistema de datos personales, del transmisor y del destinatario de los datos;
2. Finalidad de la transmisión; así como el tipo de datos que son objeto de la transmisión;
3. Las medidas de seguridad y custodia que adoptaron o fueron adoptadas por el transmisor y destinatario;
4. Plazo por el que conservará el destinatario los datos que le hayan sido transmitidos, el cual podrá ser ampliado mediante aviso al Instituto, y
5. Señalar si una vez concluidos los propósitos de la transmisión, los datos personales deberán ser destruidos o devueltos al transmisor, al igual que cualquier soporte o documento en que conste algún dato de carácter personal objeto de la transmisión.

Capítulo 4 De los informes obligatorios

Trigésimo noveno. Los responsables de los sistemas de datos personales realizarán el registro de los mismos en el Sistema "Persona" o en el que el IFAI hubiera dispuesto para este efecto, cumpliendo con los datos requeridos por el registro e informando a la Unidad

de Enlace de la actualización dentro de los primeros diez días hábiles de los meses de marzo y septiembre.

Cuadragésimo. La Unidad de Enlace informará al Comité de Información las transmisiones totales o parciales de sistemas de datos personales que realicen las áreas administrativas e investigadores del INCAR y de su notificación oportuna a través del Sistema “Persona”.

Capítulo 5 De la supervisión

Cuadragésimo primero, El Comité de Información del INCAR podrá supervisar en lo referente al cumplimiento de la protección de datos personales y a la aplicación de las medidas de seguridad establecidas a las áreas que tengan a su cargo uno varios SDP, sugiriendo en su caso, las acciones pertinentes a cada situación detectada, atendiendo en todo momento, las posibilidades de su aplicación. Las actividades de supervisión podrán realizarse de manera conjunta o solicitarse al área de Informática.

Cuadragésimo segundo. La Unidad de Enlace por instrucción del Comité de Información, dará seguimiento al cumplimiento de las sugerencias e informará de los avances.

Título II

Capítulo 1 Documento general de seguridad de los sistemas de datos personales

Cuadragésimo tercero. A fin de cumplir con las responsabilidades de la protección y resguardo de los sistemas de datos personales, en las áreas administrativas del INCAR se designará a responsable de los Sistemas de Datos Personales que coordinará cada funcionario o investigador que genere o maneje algún sistema de datos personales para el registro, reporte y control de los mismos.

Los proyectos de investigación que generen un sistema de datos personales específico, deberán contar con un responsable para efectos de cumplir los presentes Lineamientos.

Cuadragésimo cuarto. El Comité de Información del INCAR coordinará y supervisará las acciones de seguridad, disponibilidad y exactitud además de propiciar la capacitación del personal en la medida de las posibilidades.

Cuadragésimo quinto. Se destinará un espacio seguro y adecuado para la captación, manejo, tratamiento y resguardo de los sistemas de datos personales.

Capítulo 2 De la seguridad de los sistemas de datos personales

Cuadragésimo sexto. Las áreas administrativas del INCAR tomarán como guía y apoyo en materia de medidas de seguridad aplicables a los sistemas de datos personales tanto físicos como automatizados las contenidas en las Recomendaciones emitidas por el IFAI para tal efecto y los presentes Lineamientos.

Cuadragésimo séptimo. Los sistemas de datos personales relacionados o derivados de las actividades de investigación, de contratos, convenios y/o prestación de servicios estarán sujetos al menos a las medidas de seguridad establecidas en estos Lineamientos, sin menoscabo de las que se establezcan en los instrumentos legales que los respalden.

Cuadragésimo octavo. Los titulares de las áreas del INCAR y los responsables de uno o más sistemas de datos personales, deberán verificar la aplicación de las medidas de seguridad, a fin de realizar la evaluación, implementación y supervisión de ellas en sus áreas.

Capítulo 3 Medidas de seguridad

Cuadragésimo noveno. Al identificar la necesidad de crear un sistema de datos personales se designará al responsable del mismo y se comunicará al Comité de Información y a la Coordinación de Archivos en el formato SDP 1 (Anexo 1), detallando al menos los siguientes aspectos:

- Denominación del sistema de datos personales.
- Objetivo del mismo.
- Tiempo de vigencia.
- Si se relacione con un proyecto de investigación, convenio, contrato o servicio.
- Área que lo crea.
- Responsable del sistema.
- Estructura de datos.
- Áreas internas y/o personal autorizado para su manejo.
- Tipo de soporte del archivo.
- Área de resguardo.
- Formato de recopilación de información.
- Manejo externo.

Quincuagésimo. Se establecerá una bitácora de registro y seguimiento de las actividades que se realizarán con el sistema de datos personales.

Quincuagésimo primero. La bitácora de registro deberá tener hojas foliadas y rubricadas y contendrá al menos los siguientes puntos:

- Ficha de identificación del sistema con denominación, área, área de resguardo responsable y objetivo.

- Áreas internas y/o personal autorizado para su manejo.
- Actividades realizadas con fechas desde el inicio a la conclusión de la vigencia. - Incidentes o intrusiones.
- Actas.

Capítulo 4 Medidas generales de seguridad

Quincuagésimo segundo. Las medidas de seguridad mínimas aplicables estarán sustentadas en las emitidas por el IFAI en las Recomendaciones sobre Medidas de Seguridad Aplicables a los Sistemas de Datos Personales.

Capítulo 5 Medidas de seguridad mínimas aplicables al nivel básico

Quincuagésimo tercero. Las medidas de observancia obligatoria para los sistemas de datos personales en soportes físicos y automatizados serán las que se describen como aplicables al nivel básico en las Recomendaciones publicadas por el IFAI.

Quincuagésimo cuarto. Las áreas el INCAR que en el desarrollo de sus funciones requieran de recabar o mantener en custodia sistemas de datos personales en la medida de las posibilidades, procurarán contar o habilitarán un área privada o aislada para recabarlos y permitir la consulta además de habilitar mecanismos para restringir el acceso a los sistemas resguardos.

Quincuagésimo quinto. Las restricciones podrán establecerse en los manuales de procedimientos del área así como, a través de mecanismos electrónicos, sistema de vigilancia, clave de acceso, llave, entre otros.

Quincuagésimo sexto. Se deberá contar en lo posible con un registro o bitácora de las actividades, consultas y transmisiones de la información contenida en el sistema de datos personales.

CONTROL DE EMISIÓN			
	Elaboró :	**Revisó :**	**Autorizó**:
Nombre			
Firma			
Fecha			

Quincuagésimo séptimo. La subdirección de informática del INCAR opinará y actualizará las políticas y medidas técnicas específicas que se presentan en los anexos 2, 3 y 4 con la periodicidad que el cambio tecnológico y la incorporación de equipos lo requiera.

TRANSITORIOS

ARTÍCULO PRIMERO: Estos Lineamientos entrarán en vigor al día siguiente de su aprobación por el Comité de Información del INCAR.

ARTÍCULO SEGUNDO: El área de Informática emitirá las políticas específicas, los manuales de operación y los difundirá en los ciento ochenta días siguientes a la autorización de los presentes Lineamientos.

ARTÍCULO TERCERO: Los presentes Lineamientos se actualizarán de acuerdo a las recomendaciones sobre los estándares mínimos de seguridad aplicables a los sistemas de datos personales que emita el IFAI.

ARTÍCULO CUARTO: Los casos no previstos en estos Lineamientos serán resueltos por el Comité de Información del INCAR.

ARTÍCULO QUINTO: Los presentes Lineamientos de Protección y Seguridad de los Sistemas de Datos Personales del INCAR necesitan para su adopción definitiva de la autorización de la Junta de Gobierno del Instituto.

CONTROL DE EMISIÓN			
	Elaboró :	**Revisó :**	**Autorizó**:
Nombre			
Firma			
Fecha			

ANEXO 1

Registro de Sistema de Datos Personales

- Denominación
- Objetivo
- Proyecto de investigación
- Núm. registro del proyecto
- Convenio Institución (es) participante (s)
- Contrato Empresa (s) o agencia (s)
- Servicio Función o atribución Otro (especificar)
- Área responsable
- Responsable del Sistema
- Tipo de datos
- Manejo
- Transmisión Nivel de seguridad
    - Sí No Básico Medio Alto
- Total de registros
- Tiempo de vigencia
- Tipo de soporte
    - Físico
    - Automatizado
    - Relacionado a biobanco
    - Otro (especificar)
- Área de resguardo
- Modalidad de autorización
- Consentimiento informado
- Formato de recopilación o entrevista
- Otro (especificar)
- Personal autorizado

CONTROL DE EMISIÓN			
	Elaboró :	**Revisó :**	**Autorizó**:
Nombre			
Firma			
Fecha			

- Director del Área Responsable del SDP
  - Nombre y firma
- Fecha Lineamientos Protección y Seguridad de los Sistemas de Datos Personales del Instituto Nacional de Cardiología Ignacio Chávez.

CONTROL DE EMISIÓN			
	Elaboró :	**Revisó :**	**Autorizó**:
Nombre			
Firma			
Fecha			

ANEXO 2

Medidas generales de seguridad del nivel básico

1. Área de recepción de datos personales

a. Privada para garantizar la confidencialidad.
b. Infraestructura apropiada, los procesos y procedimientos para mantener en forma organizada y segura los datos recabados, previo a las fases de tratamiento.
c. El personal autorizado con identificación oficial emitida por el INCAR.
d. En caso necesario, señalización visible sobre las prohibiciones que aplican y restricciones de acceso.
e. Dar aviso al personal de vigilancia en caso de sospecharse la presencia de personas no autorizadas en el área.

2. Área de resguardo de datos personales

a. Infraestructura y mobiliario apropiados para contener los sistemas de datos personales a fin de mantenerlos en forma organizada y segura además, protegidos de condiciones adversas, humedad, temperatura, iluminación solar, polvo, consumo de alimentos y presencia de plagas, entre otras.
b. Condiciones ambientales que permitan preservar en buen estado los soportes físicos durante el tiempo de conservación establecido.
c. Puerta de acceso con cerradura u otra tecnología que impida la libre apertura.
d. Cerrada en horas no hábiles y/o cuando el personal no esté presente.
e. El personal autorizado con identificación oficial emitida por el INCAR.
f. Existe señalización sobre las restricciones de acceso, las prohibiciones que aplican y el procedimiento para dar aviso al personal de vigilancia en caso de sospecharse la presencia de personas no autorizadas.

3. **Área de consulta de datos personales**
    a. Infraestructura apropiada, procesos y procedimientos suficientes para supervisar y vigilar los soportes físicos que consultan los Usuarios dentro del área.
    b. El personal autorizado con identificación oficial emitida por el INCAR.
    c. Señalización visible con horarios de atención, restricciones de acceso, prohibiciones y el procedimiento para dar aviso al personal de vigilancia en caso de sospecharse la presencia de personas no autorizadas en el área.
4. **Acceso y consulta de datos personales**
    a. **Acceso**
        i. Revisión por el personal de vigilancia para control del acceso y verificación de la identidad de quienes tienen el propósito de ingresar.
        ii. El Encargado de los SDP's es el único que autoriza la entrada al personal debidamente registrado, anotando el hecho en la bitácora.
        iii. Medidas de seguridad para el ingreso a una zona de acceso restringido.
    b. **Consulta**
        i. El Encargado de los SDP's al autorizar la salida de datos personales en soportes en soportes físicos, anotará el hecho en la bitácora correspondiente.
    c. **Personas autorizadas y no autorizadas**
        i. El Encargado de los SDP's autorizará el ingreso a las zonas de acceso restringido donde existen datos personales en soportes físicos.
    d. **Medidas para la prevención de intrusiones**
        i. El personal autorizado que labora en las zonas de los SDP's verifica durante el desempeño de sus funciones que no hay personas no autorizadas.

e. **Registro de actividades**

i. Operación cotidiana

1. El Responsable de los SDP's mantiene estricto control y registro de:
    a. Las autorizaciones para interactuar con uno o más SDP's, ya sea en el área de consulta o desde otro lugar distinto.
    b. La asignación, actualización y reemplazo de llaves, tarjetas, contraseñas de acceso y demás elementos que entregue para ingresar a las zonas restringidas.
    c. Las autorizaciones emitidas a los usuarios y demás personal debidamente registrado que solicitan acceso a las áreas de recepción o resguardo. Para ello, el Encargado anota:
        i. Nombre de la persona quién solicita el acceso.
        ii. Fecha en la que lo solicita
        iii. Fecha en que se realiza el acceso
        iv. La razón que lo motiva.
    d. Las autorizaciones emitidas a los usuarios que solicitan permiso para extraer datos personales en soportes físicos. Para ello, el Encargado registra:
        i. Nombre de la persona quién solicita el acceso
        ii. Qué documentos se lleva
        iii. Fecha en que se realiza el acceso
        iv. Fecha en que se compromete a devolverlos (si aplica)
        v. Fecha en que efectivamente los devuelve (si aplica).

e. Las autorizaciones emitidas a los usuarios que solicitan permiso para introducir equipo de cómputo o de conexión inalámbrica u otro similar a las zonas de acceso restringido. Para ello, el Encargado registra: -

i. Nombre de la persona quien solicita el acceso
ii. Qué equipo introducirá
iii. Cuándo y por cuánto tiempo

5. Divulgación de incidentes En caso de presentarse un incidente, se continúa con el siguiente procedimiento:

a. El responsable del personal de vigilancia emite un informe al Responsable de los SDP's a no más de 3 días naturales de haber ocurrido el incidente.

b. En caso de robo o extravío de datos personales en soportes físicos, el titular del área administrativa y/o el Responsable de los SDP's, al tener conocimiento del incidente, hace de conocimiento de la Dirección General, del Órgano Interno de Control y del área de Asuntos Jurídicos en términos del Estatuto Orgánico, para que cada uno, en el ámbito de sus atribuciones, determine lo conducente.

c. En caso de robo o extravío de datos personales, se alerta a los titulares de los datos afectados para que tomen sus precauciones ante el posible uso ilegal de su información. Para tal efecto, el Responsable de los SDP's del área da aviso por escrito a dichos titulares, a más tardar cinco días naturales de haber ocurrido el incidente, recabando el acuse de recibo de esta notificación. Con anticipación a dicho escrito, si se cuentan con los datos actualizados, se da aviso por correo electrónico (solicitando acuse de recibido) o por teléfono.

6. Supervisión

a. 1. El Comité de Información del INCAR establecerá un calendario para la realización de una supervisión interna a las unidades administrativas que mantienen y operan SDP's.

7. **Baja de datos personales** Para proceder a la baja documental de soportes físicos que contienen datos personales, deberán observarse las disposiciones establecidas por el Capítulo III De la Conservación de Archivos, de los Lineamientos Generales para la Organización y Conservación de los archivos de las dependencias y entidades de la Administración Pública Federal (D.O.F 20/02/04), lo establecido en el capítulo X de los Lineamientos de Organización y Conservación de Archivos del INCAR y además el encargado de los SDP's:
    a. Destruye por completo dichos soportes físicos antes de desecharlos.
    b. Lleva una bitácora de las veces que se efectúa la acción de baja de datos personales.
    c. Los métodos de destrucción de datos personales en soportes físicos están definidos en el Los Lineamientos de Organización y Conservación de Archivos y en los Lineamientos de Protección de Datos Personales del INCAR y su correcta aplicación es responsabilidad tanto del titular del área como del Responsable de los SDP's antes de ejecutarlos.
    d. Cuando se realice la separación de materiales para su reciclaje (como podría suceder con el papel, el cartón, el metal y el plástico), los datos personales contenidos en materiales reciclables deberán ser triturados y la viruta resultante se entrega directamente a una empresa o entidad que los recibe para procesarlos de inmediato, solicitando una garantía por escrito que no serán examinados para su eventual reconstrucción.

8. **MS para datos personales en soportes electrónicos**
    a. **Área de recepción de datos personales**
        i. Existe la infraestructura apropiada y se siguen los procesos y procedimientos necesarios para mantener en forma organizada y segura los datos personales recibidos en el área, en tanto siguen la demás fases de su tratamiento.

ii. El equipo de cómputo instalado en el área de recepción cumple con las Recomendaciones presentadas en la sección “4. MS para equipo de cómputo en zonas de acceso restringido” de los Lineamientos del IFAI y las que sean establecidas por el área de Informática del INCAR.

iii. Dicho equipo de cómputo está provisto de la tecnología necesaria y suficiente para verificar la identidad del personal autorizado que labora en el área de recepción.

iv. El personal ostenta una identificación oficial emitida por el INCAR.

v. Existe señalización visible sobre las restricciones de acceso, las prohibiciones que aplican y el procedimiento para dar aviso al personal de vigilancia en caso de sospecharse la presencia de personas no autorizadas en el área.

9. Área de resguardo de datos personales

a. Los archivos que contengan datos personales preferentemente se resguardarán en áreas de acceso restringido.

b. Existe la infraestructura apropiada y se siguen los procesos y procedimientos necesarios y suficientes para mantener en forma organizada y segura los datos personales en soportes electrónicos dentro del área de resguardo.

c. Al interior del área de resguardo, existen las condiciones ambientales idóneas para preservar en buen estado los datos personales en soportes electrónicos durante el tiempo definido de conservación.

d. La puerta de acceso del área de resguardo cuenta con cerradura, dispositivo electrónico o cualquier otra tecnología que impida su libre apertura. Este mecanismo queda cerrado en horas no hábiles o cuando el personal autorizado que ahí labora abandona el área.

e. El equipo de cómputo instalado en el área de resguardo cumple con las Recomendaciones presentadas en la sección “MS para equipo de cómputo en zonas de acceso restringido”.

f. El mobiliario utilizado dentro del área de resguardo protege los datos personales en soportes electrónicos de condiciones adversas en humedad, temperatura, iluminación solar, polvo, consumo de alimentos y presencia de plagas, entre otras.

g. El mobiliario utilizado para almacenar los datos personales en soportes electrónicos cuenta con cerraduras, dispositivos electrónicos o cualquier otra tecnología que impida la libre apertura de sus puertas, cajones o compartimientos. Tales mecanismos quedan cerrados en horas no hábiles.

h. El personal autorizado que labora en el área de resguardo ostenta una identificación con fotografía (credencial o gafete) emitida por el INCAR.

i. No está permitido el libre acceso y el uso de aquellos aparatos referidos en la sección “Equipo no autorizado” de los Lineamientos del IFAI y las que sean establecidas por el área de Informática del INCAR.

j. Existe señalización visible sobre las restricciones de acceso, las prohibiciones que aplican y el procedimiento para dar aviso al personal de vigilancia en caso de sospecharse la presencia de personas no autorizadas en el área de resguardo.

10. Área de consulta de datos personales

a. Existe la infraestructura apropiada y se siguen los procesos y procedimientos necesarios y suficientes para supervisar y vigilar los datos personales en soportes electrónicos que consultan los Usuarios de los datos.

b. El equipo de cómputo instalado en el área de consulta cumple con las Recomendaciones presentadas en la sección “4. MS para equipo de cómputo en zonas de acceso restringido” de los Lineamientos del IFAI y las que sean establecidas por el área de Informática del INCAR. 3. El usuario que labora en el área ostenta una identificación oficial emitida por el INCAR. 4. Existe señalización visible sobre: horarios de atención, restricciones de acceso, prohibiciones que aplican y el procedimiento para dar aviso al personal de vigilancia en caso de sospecharse la presencia de personas no autorizadas.

11. Acceso y consulta de datos personales

a. **Acceso**

i. El acceso a las áreas, mobiliario, equipos de cómputo o archiveros en donde están contenidos los sistemas en soportes físicos, el personal vigila, controla el acceso y verifica la identidad de quienes tienen el propósito de ingresar a dicha zona.

ii. El encargado de los SDP's es el único que autoriza la entrada las áreas de recepción y de resguardo al personal debidamente registrado, anotando el hecho en la bitácora.

iii. En todo caso, el INCAR adoptará las medidas de seguridad necesarias, en la medida de sus posibilidades para el ingreso a una zona de acceso restringido.

b. **Consulta**

i. El Encargado de los SDP's al autorizar la salida de datos personales en soportes en soportes físicos, anota el hecho en la bitácora de actividades ("2.5. Registro de actividades") de los Lineamientos del IFAI y las que sean establecidas por el área de Informática del INCAR.

c. **Personas autorizadas y no autorizadas**

i. El ingreso a las zonas de acceso restringido donde existen datos personales en soportes electrónicos es sólo con la autorización del Responsable de los mismos.

ii. Cada acceso y consulta realizada por personas no autorizadas será considerada como un incidente de intrusión que se denuncia ante las autoridades competentes para su investigación.

d. **Medidas para la prevención de intrusiones**

i. El personal autorizado que labora en las zonas de acceso restringido de los SDP's verifica durante el desempeño de sus funciones que en dichas áreas no hay personas no autorizadas.

ii. El equipo de cómputo instalado en las zonas de acceso restringido cumple con las Recomendaciones presentadas en la sección “4. MS para equipo de cómputo en zonas de acceso restringido”.

e. **Registro de actividades**

i. **Operación cotidiana** El Responsable de los SDP’s establece una bitácora de actividades y mantiene estricto control y registro de:

1. Las autorizaciones emitidas para facultar a un servidor público como usuario para interactuar con uno o más SDP’s, acudiendo al área o fuera de dicha área.
2. La asignación, actualización y reemplazo de llaves, tarjetas, contraseñas de acceso y demás elementos que entregue a los usuarios para el acceso.
3. Las autorizaciones emitidas a los usuarios y demás personal que solicitan acceso a las áreas de recepción o resguardo. Para ello, el Encargado registra: - Quién solicita el acceso. - Cuándo lo solicita. - Cuándo se lleva a cabo. - La razón que lo motiva.
4. Las autorizaciones emitidas a los usuarios que solicitan permiso para extraer datos personales en soportes electrónicos del área de consulta. Para ello, el Encargado registra: - Quién hace la solicitud. - Qué documentos se lleva y en qué tipo de soporte (físico o electrónico). - Cuándo se los lleva. - Cuándo promete devolverlos (si aplica). - Cuándo efectivamente los devuelve (si aplica).
5. Las autorizaciones emitidas a los usuarios que solicitan permiso para introducir aparatos tales como los mencionados en la sección “. Equipo no autorizado” de los Lineamientos del IFAI y las que sean establecidas por el área de Informática del INCAR. Para ello, el Encargado registra: - Quién hace la solicitud. - Qué equipo introducirá. - Cuándo y por cuánto tiempo.

f. **Divulgación de incidentes** En caso de presentarse un incidente o en caso de robo o extravío de datos personales en soportes electrónicos, se sigue el procedimiento el siguiente proceso al tener conocimiento del hecho:

   i. El responsable del personal de vigilancia emite un informe al Responsable de los SDP's a no más de 3 días naturales de haber ocurrido el incidente.
   ii. El responsable realizar la anotación correspondiente en la bitácora.
   iii. Levantar un acta circunstanciada en presencia del responsable de los SDP's, con representantes del Coordinador de Archivos, Asuntos Jurídicos, Comité de Información y el Órgano Interno de Control, a quienes se entregará una copia del documento.
   iv. En caso de robo o extravío, se alerta a los titulares de los datos afectados para que tomen sus precauciones ante el posible uso ilegal de su información.
   v. El Responsable de los SDP's da aviso por escrito a los titulares de los datos personales, a más tardar cinco días naturales, recabando el acuse de recibo de esta notificación. Con anticipación a dicho escrito, si se cuentan con los datos actualizados, se da aviso por correo electrónico o por teléfono.

g. **Supervisión** El Comité de información del INCAR propone la realización de una supervisión interna para las unidades administrativas que mantienen y operan SDP's así como para los terceros contratados que interactúan con dichos SDP's.

h. **Baja de datos personales** Para proceder a la baja documental de soportes electrónicos que contienen datos personales, deberán observarse las disposiciones establecidas por el Capítulo III De la Conservación de Archivos, de los Lineamientos Generales para la organización y conservación de los archivos de las dependencias y entidades de la Administración Pública Federal (D.O.F 20/02/04), y además:

i. Todo soporte electrónico que será dado de baja (ya sea por obsolescencia, sustitución o alguna otra causa) pasa por un proceso de preparación final antes de ser desechado. Dicho proceso incluye: la transferencia del contenido que sea preciso conservar hacia otro soporte electrónico y la destrucción, inhabilitación o daño que deje inservible dicho soporte.

ii. Las únicas personas autorizadas para realizar proceso de preparación final son el área de sistemas y el personal de vigilancia en presencia del responsable de SDP y procediendo a levantar el acta circunstanciada correspondiente.

iii. Los métodos de destrucción de datos personales en soportes electrónicos serán definidos por el área de Informática; o, si no lo están, son aprobados por el responsable de los SDP's antes de ejecutarlos.

iv. El encargado de los SDP's: a) Vigila que se sigan los procedimientos y se utilicen los mecanismos para asegurar la destrucción de soportes electrónicos. b) Lleva una bitácora donde registra la baja de soportes electrónicos que contienen datos personales anotando: - Nombre y firma de la persona que realiza esta acción. - Fecha y hora en la que se realiza. - El destino que se le dará al soporte electrónico desechado. - Nombre y firma (visto bueno) del Responsable de los SDP's.

i. **MS para transmisión de datos personales**

i. **Transmisión de datos personales en soportes físicos**

1. **Transmisión mediante traslado físico**

a. La transmisión de datos personales en soportes físicos al interior del INCAR se realiza mediante la vía elegida, de común acuerdo, entre las partes: mensajero interno, asistente secretarial, visita personal, etc.

b. La transmisión al exterior se realiza mediante un servicio de mensajería externo. En este caso, se define un

destinatario primario y otro secundario por si el mensajero no encuentra al primero.

c. El paquete con datos personales en soportes físicos viaja debidamente sellado, de forma tal que sea perceptible cualquier violación o apertura no autorizada.

ii. **Transmisión de datos personales en soportes electrónicos**

1. **Preparación previa a la transmisión**

a. Los datos personales que son enviados a un destinatario autorizado para manipularlos o procesarlos son sometidos a un proceso de preparación previa a la transmisión. En este caso, el encargado que realiza dicho proceso: **-** Genera archivos electrónicos que contengan los datos personales solicitados en un formato que permita al destinatario efectuar las operaciones que requiera.

b. Los datos personales que son enviados a un destinatario con autorización para manipularlos o procesarlos no son reintegrados al SDP de donde fueron extraídos, a menos que el destinatario haya efectuado una corrección solicitada por el titular de los datos. **-** Los datos personales que son enviados a un destinatario No autorizado para manipularlos o procesarlos son sometidos a un proceso distinto de preparación previa a la transmisión.

2. **Transmisión mediante traslado físico**

a. La transmisión de datos personales en soportes electrónicos al interior de INCAR se realiza mediante la vía elegida, de común acuerdo, entre las partes:

mensajero interno, asistente secretarial, visita personal, etc.

b. El paquete con datos personales en soportes electrónicos viaja debidamente sellado, de forma tal que sea perceptible cualquier violación o apertura no autorizada del mismo. Dichos soportes electrónicos contienen los archivos electrónicos resultantes del proceso de preparación previa a la transmisión.

3. **Transmisión mediante redes de comunicación electrónica**
   a. La transmisión de datos personales en archivos electrónicos, previamente preparados para su transmisión, se realiza mediante redes de comunicación electrónica.
4. **Medidas para la prevención de intrusiones desde el exterior**
   a. Existen dispositivos de la más alta seguridad posible instalados en caso de que la red de comunicación electrónica (que conecta los servidores que contienen los datos personales con las computadoras que se utilizan para acceder a ellos) esté conectada a Internet.
5. **Registro de actividades**
   a. **Operación cotidiana**
      i. El Encargado de los SDP's mantiene estricto control y registro de: a) Las autorizaciones emitidas a destinatarios que han solicitado que los datos personales en soportes electrónicos les sean transmitidos en un formato que permita manipularlos o procesarlos. b) Todas las transmisiones efectuadas, para ello, anota los datos necesarios para emitir informes sobre la

transmisión según el lineamiento vigésimo sexto de los Lineamientos de Protección de Datos Personales publicados en el Diario Oficial de la Federación el 30 de septiembre de 2005.

6. **Divulgación de incidentes**

   a. En caso de presentarse un incidente, se sigue el procedimiento que esa dependencia o entidad tenga definido.

   b. En caso de que dicho procedimiento no lo incluya, además, se llevan a cabo las siguientes actividades, sin necesidad de que se realicen en el orden que aparecen:

   c. El responsable del personal de vigilancia emite un informe al Responsable de los SDP's a no más de 3 días naturales de haber ocurrido el incidente.

   d. En caso de robo o extravío de datos personales en soportes físicos, el Director General, los titulares de las áreas administrativas del INCAR o el Responsable de los SDP's, al tener conocimiento del incidente, da vista al Órgano Interno de Control, al área jurídica y/o al servidor público que tenga facultades para presentar denuncias o querellas de cada dependencia o entidad, en términos del Estatuto Orgánico, según corresponda, para que cada uno, en el ámbito de sus atribuciones, determine lo conducente.

   e. En caso de robo o extravío de datos personales, se alerta a los titulares de los datos afectados para que tomen sus precauciones ante el posible uso ilegal de su identidad. Para tal efecto, el Responsable de los SDP's da aviso por escrito a dichos titulares, a más tardar cinco

días naturales de haber ocurrido el incidente, recabando el acuse de recibo de esta notificación. Con anticipación a dicho escrito, si se cuentan con los datos actualizados, se da aviso por correo electrónico o por teléfono.

7. **Supervisión** El Comité de información del INCAR propone la realización de una supervisión a las unidades administrativas que mantienen y operan SDP's así como a los terceros contratados.

j. **MS para equipo de cómputo en zonas de acceso restringido**

i. **Computadoras de escritorio**

1. **Recepción**

a. Una computadora de escritorio asignada para uso en zonas de acceso restringido, sea nueva o usada, pasa por un *proceso de preparación inicial* a fin de instalarle solamente software autorizado, configurado para brindar mayor seguridad que la predeterminada por el fabricante.

b. El proceso de preparación inicial de la computadora de escritorio incluye, antes de instalar el software, sobrescribir con un solo valor (unos o ceros) el 100% del medio principal de almacenamiento no volátil con alguna herramienta especializada.

c. La lista de software autorizado para computadoras de escritorio en sitios de acceso restringido es un documento que prepara y actualiza el área de Informática del INCAR. Este documento se prepara en coordinación con los responsables de los SDP's además se informa a la Unidad de Enlace y al Comité de

Información, según las necesidades y las funciones que desempeña el personal autorizado.

d. El encargado de los SDP's supervisa y verifica que la computadora de escritorio cumpla con los requerimientos de instalación establecidos y las configuraciones de seguridad definidas.

e. El proceso de preparación inicial de una computadora de escritorio que se asigna en zonas de acceso restringido queda registrado en un formulario. Este documento es archivado por el área de Informática.

2. **Resguardo** La computadora de escritorio está asegurada físicamente para evitar el robo del gabinete o la sustracción de piezas o partes. Para tal propósito, está resguardada con cajones de protección, candados o cualquier otro dispositivo que impida la manipulación del gabinete y el acceso físico al interior del equipo.

3. **Operación**

a. Están deshabilitados (en el interior del equipo) o cancelados (en el exterior) los puertos de comunicación (USB, paralelo, serial, etc.) que no se utilizan. Los cables o dispositivos conectados a los puertos que sí se utilizan están asegurados para evitar su desconexión. Las cancelaciones pueden ser abiertas por personal autorizado del área de sistemas.

b. El acceso a una computadora de escritorio dentro de una zona de acceso restringido, con el propósito de realizar labores de mantenimiento preventivo y correctivo o para soporte técnico, es exclusivo para el personal de Informática o un proveedor externo. En cualquier caso, el

responsable de los SDP's es quien autoriza, supervisa y registra el acceso archivando la autorización que emite.

4. **Atención de fallas**
    a. Cuando se presenta una falla en una computadora, el usuario del equipo o, en su caso, el responsable de los SDP's reporta de inmediato el evento al área de Informática y, toma las primeras acciones para evitar el deterioro del equipo siguiendo las indicaciones que reciba del personal de Informática.
    b. En caso de que la falla requiera que la computadora sea retirada para su reparación, los medios de almacenamiento no volátil son extraídos y puestos a resguardo para evitar la pérdida, robo o daño de los datos personales.
5. **Baja**
    a. Toda computadora que es dada de baja (ya sea por obsolescencia, sustitución o alguna otra causa) pasa por un proceso de preparación final.
    b. El proceso de preparación final incluye transferir a otro equipo los archivos que contengan información que sea preciso conservar y sobrescribir con un solo valor (unos o ceros) el 100% de los medios de almacenamiento no volátil con alguna herramienta especializada para ello.
    c. Las únicas personas autorizadas para realizar el proceso de preparación final son miembros del personal de informática y de vigilancia.
    d. El proceso de preparación final de una computadora que se da de baja queda registrado en un formulario. Este documento es archivado por el área de informática con

el formulario en que se registró el proceso de preparación inicial.

ii. **Servidores**

1. **Recepción**

a. Un servidor asignado para uso en zonas de acceso restringido, sea nuevo o usado, pasa por un proceso de preparación inicial a fin de instalarle solamente software autorizado, configurado para brindar la mayor seguridad posible.

b. El proceso de preparación inicial del servidor incluye, antes de instalar el software, sobrescribir con un solo valor (unos o ceros) el 100% de los medios principales de almacenamiento no volátil con alguna herramienta especializada para ello.

c. La lista de software autorizado para servidores en sitios de acceso restringido es un documento que prepara y actualiza el área de sistemas del INCAR. Este documento se prepara en coordinación con el responsable de los SDP's, según las necesidades y las funciones que desempeña el personal autorizado a su cargo.

d. Las únicas personas autorizadas para realizar el proceso de preparación inicial son miembros del personal de las áreas de sistemas o de vigilancia.

e. El encargado supervisa y verifica que el servidor cumpla con los requerimientos de instalación y las configuraciones de seguridad definidas.

f. El proceso de preparación inicial de un servidor que se asigna en zonas de acceso restringido queda registrado

en un formulario. Este documento es archivado por el área de Informática o por el personal de vigilancia.

2. **Resguardo**
    a. Todo servidor que está bajo la custodia del área de sistemas está instalado en un lugar que facilita adoptar: - Medidas de seguridad. - Medidas para su buen funcionamiento. - Medidas que aseguran su operación continua.
    b. Todo el equipo y servidores estarán bajo la custodia del área de Informática y asegurado físicamente para evitar el robo del gabinete o la sustracción de piezas o partes. Para tal propósito, está resguardado mediante cualquier otro dispositivo que impida la manipulación del gabinete y el acceso físico al interior del equipo.
3. **Operación**
    a. Si el servidor que No está bajo la custodia del área de Informática tiene deshabilitados o cancelados los puertos de comunicación (USB, paralelo, serial, etc.) que no se utilizan. Los cables o dispositivos conectados a los puertos que sí se utilizan están asegurados para evitar su desconexión. Las cancelaciones pueden ser abiertas por personal de sistemas.
    b. Aquel servidor que No está bajo la custodia del área de Informática tiene deshabilitados o cancelados los dispositivos de almacenamiento removible (unidades de disco flexible, quemadores de CD/DVD, etc.). Las cancelaciones pueden ser abiertas por personal de sistemas.

c. No existen dispositivos de conexión inalámbrica (Wi-Fi, Bluetooth, infrarrojo, etc,) en los servidores asignados dentro de las zonas de acceso restringido de los SDP's ni en aquellos que están bajo la custodia del área de sistemas.

d. El acceso a un servidor que No está bajo la custodia del área de Informática, con el propósito de realizar labores de mantenimiento preventivo y correctivo o para soporte técnico, es exclusivo para el personal de sistemas o para un proveedor externo subcontratado. En cualquier caso, el encargado de los SDP's es quien autoriza, supervisa y registra el acceso, archivando la autorización que emite.

4. **Atención de fallas**

a. Cuando se presenta una falla en un servidor que No está bajo la custodia del área de Informática, el responsable de los SDP's reporta de inmediato el evento y, de ser posible, toma las primeras acciones para evitar un mayor deterioro del equipo siguiendo las indicaciones que reciba.

b. Para los servidores críticos que están bajo la custodia del área de Informática, dicha área contratará en la medida de lo posible una póliza de reparación, mantenimiento preventivo y correctivo cuyo tiempo de respuesta es suficiente para atender la criticidad de la información contenida en el equipo.

c. En caso de que la falla requiera que el servidor sea retirado de las zonas de acceso restringido para su reparación, los medios de almacenamiento no volátil son extraídos y puestos a resguardo para evitar la pérdida,

robo o daño de los datos personales que contiene. Dicha operación la realiza el personal autorizado.

5. **Baja**
    a. Todo servidor que es dado de baja (ya sea por obsolescencia, sustitución o alguna otra causa) pasa por un proceso de preparación final.
    b. El proceso de preparación final incluye transferir a otro equipo los archivos que contengan información que sea preciso conservar y sobrescribir con un solo valor (unos o ceros) el 100% de los medios de almacenamiento no volátil con alguna herramienta especializada para ello.
    c. Las únicas personas autorizadas para realizar el proceso de preparación final son miembros del personal de las áreas de Informática.
    d. El proceso de preparación final de un servidor que se da de baja queda registrado en un formulario. Este documento es archivado por el área de Informática con el formulario que en su momento registró el proceso inicial del equipo.

iii. **Impresoras y otros equipos periféricos autorizados**

1. **Recepción** Las impresoras y los equipos periféricos autorizados (monitores, pantallas planas, etc.) usados en las zonas de acceso restringido de un SDP, sean nuevos o usados, pasan por un proceso de preparación inicial.
2. **Atención de fallas**
    a. Cuando se presenta una falla en una impresora o en un equipo periférico autorizado, el usuario del equipo o, en su caso, el responsable de los SDP's reporta de inmediato el evento al área de Informática y, de ser

posible, toma las primeras acciones para evitar un mayor deterioro siguiendo las indicaciones que reciba.

b. En caso de que la falla requiera que la impresora o el equipo periférico autorizado sea retirado de las zonas de acceso restringido de los SDP's para su reparación, de existir medios de almacenamiento no volátil, estos son extraídos y puestos a resguardo para evitar la pérdida, robo o daño de datos personales. Dicha operación la realiza el personal autorizado del área de Informática.

3. **Baja**

a. Toda impresora y todo equipo periférico autorizado que son dados de baja (ya sea por obsolescencia, sustitución o alguna otra causa) pasan por un proceso de preparación final definido por el área de Tecnologías de la Información en caso necesario.

b. El proceso de preparación final de una impresora o de un equipo periférico autorizado que se da de baja queda registrado. Este documento es archivado por el área de Informática y se archiva con el formulario que en su momento registró el proceso de preparación inicial del equipo.

iv. **Registro de actividades e inventario**

1. **Control de activos (inventarios)** El área de Informática lleva un inventario actualizado (independiente de aquél que lleva el área administrativa) para todos los activos de cómputo, separados por tipo; es decir, computadoras personales, servidores, impresoras y equipos periféricos autorizados.

v. **Operación cotidiana**

1. El Responsable de los SDP's mantiene estricto control y registro de:
   a. Las autorizaciones emitidas al personal de Informática o a proveedores externos que proporcionan servicios de mantenimiento preventivo y correctivo así como soporte técnico en áreas de acceso restringido. Dicho registro se lleva a cabo por el encargado e incluye, por lo menos, los siguientes datos: **-** Causa que motiva el servicio. **-** Número o identificación de activo del equipo de cómputo. **-** Fecha y hora, tanto de inicio como de terminación del servicio. **-** Nombre completo y firma quien proporciona el servicio. **-** Tipo de identificación oficial que utiliza(n) dicha(s) persona(s) para acreditar su identidad (credencial de elector, pasaporte, etc.) y un número de referencia que aparezca en dicha identificación. **-** Nombre y firma del responsable que autoriza el acceso.
   b. Las autorizaciones para la operación de equipo de almacenamiento removible externo por parte del personal de sistemas o de vigilancia cuando es necesario llevar a cabo respaldos de información contenida en computadoras de escritorio o servidores que No están bajo la custodia del área de sistemas.
   c. Las autorizaciones para el uso temporal de dispositivos como los que se listan en la sección "Equipo no autorizado" de los Lineamientos del IFAI y las que sean establecidas por el área de Informática del INCAR que se otorgan al personal autorizado que así lo solicite. Dicho registro incluye, por lo menos, los siguientes datos

y documentos: - Causa que motiva la solicitud. - Nombre completo de la persona que solicita autorización. - Fecha en la que obtuvo autorización para interactuar con uno o más SDP's, nombre del responsable de los SDP's que otorgó dicha autorización y fotocopia del documento que le otorgó la categoría de personal autorizado. Tipo de identificación oficial con la que dicha persona acredita su identidad (credencial de elector, pasaporte, etc.) y un número de referencia que aparezca en tal identificación. - Nombre y firma (visto bueno) del Responsable de los SDP's que autoriza el acceso. - En forma opcional, se toma fotografía de la persona que obtiene acceso y del equipo no autorizado que utilizará en zonas de acceso restringido. - Carta responsiva emitida por el usuario, encargado o demás personal que incluye su firma autógrafa y un manifiesto en el que asume la responsabilidad por el daño, pérdida o robo de los datos personales que almacene en el equipo no autorizado que utilice temporalmente en cualesquiera de las zonas de acceso restringido de los SDP's. 2. El área de sistemas o el personal de vigilancia mantiene estricto control y registro de:

i. El formulario donde se asientan los detalles del proceso de preparación inicial que se lleva a cabo para cada computadora de escritorio y cada servidor asignado en áreas de acceso restringido. Dicho registro incluye, por lo menos, los siguientes datos: **-** Nombre y firma de la o las personas que realizan el proceso de preparación

inicial. **-** Fecha y hora en la que se realiza dicho proceso, tanto la de inicio como la de finalización. **-** Características del equipo (marca, modelo y número de serie) así como de los componentes de hardware al interior del equipo (marca y modelo de la unidad de procesamiento central; marca y cantidad de la memoria volátil; marca, modelo y capacidad de los medios de almacenamiento no volátil; marca y versión del sistema operativo instalado; y demás componentes relevantes) en el momento de su recepción. **-** Nombre y firma (visto bueno) dado por el Responsable de los SDP's. **-** Número o identificación de activo del equipo que se asigna al equipo. **-** Fecha en que el equipo queda instalado y se pone en operación. **-** Área donde queda instalado el equipo.

ii. El formulario donde se asientan los detalles del proceso de preparación inicial que se lleva a cabo para cada impresora y cada equipo periférico autorizado asignado en áreas de acceso restringido. Dicho registro incluye, por lo menos, los siguientes datos: - Nombre y firma de la o las personas que realizan el proceso de preparación inicial. - Fecha y hora en la que se realiza dicho proceso, tanto la de inicio como la de finalización. - Características del equipo (marca, modelo y número de serie) así como de los componentes de hardware al interior del

equipo (marca y cantidad de la memoria volátil; marca, modelo y capacidad de los medios de almacenamiento no volátil; y demás componentes relevantes) en el momento de su recepción. - Nombre y firma (visto bueno) dado por el Responsable de los SDP's. - Número o identificación de activo del equipo que se asigna al equipo. - Fecha en que el equipo queda instalado y se pone en operación.

iii. El inventario actualizado de activos de cómputo, mismo que incluye, por lo menos, los siguientes datos: **-** Descripción. **-** Área donde se instaló el equipo. **-** Número o identificación de activo que el equipo de cómputo tenía asignado. **-** Características del equipo (marca, modelo y número de serie). **-** Características de los componentes de hardware al interior del equipo (marca y modelo de la unidad de procesamiento central; marca y cantidad de la memoria volátil; marca, modelo y capacidad de los medios de almacenamiento no volátil; marca y versión del sistema operativo instalado; y demás componentes relevantes) en el momento de su recepción. **-** Características de los componentes de hardware al interior del equipo (marca y modelo de la unidad de procesamiento central; marca y cantidad de la memoria volátil; marca, modelo y capacidad de los medios de almacenamiento no volátil; marca y versión del

sistema operativo instalado; y demás componentes relevantes) en el momento de su baja. **-** Memoria técnica de las configuraciones de red del equipo, si aplica. **-** Folio del formulario que registra los detalles del proceso de preparación inicial y fecha de alta en el inventario. **-** Folio del formulario que registra los detalles del proceso de preparación final y fecha de baja del inventario.

iv. El formulario donde se asientan los detalles del proceso de preparación final que se lleva a cabo para cada computadora de escritorio y cada servidor asignado en áreas de acceso restringido. Dicho registro incluye, por lo menos, los siguientes datos: - Área donde estaba instalado el equipo. - Número o identificación de activo que el equipo de cómputo tenía asignado. - Nombre y firma de la persona que realiza el proceso de preparación final. - Fecha y hora en la que se realiza dicho proceso, tanto la de inicio como la de finalización. - Características del equipo (marca, modelo y número de serie) así como de los componentes de hardware al interior del equipo (marca y modelo de la unidad de procesamiento central; marca y cantidad de la memoria volátil; marca, modelo y capacidad de los medios de almacenamiento no volátil; marca y versión del sistema operativo instalado; y demás componentes relevantes) en el momento de su baja. - El destino que se le dará al equipo dado

de baja. - Fecha en la que el equipo es efectivamente dado de baja. - Nombre y firma (visto bueno) del Responsable de los SDP's.

v. El formulario donde se asientan los resultados del proceso de preparación final que se lleva a cabo para cada impresora y cada equipo periférico autorizado asignado en áreas de acceso restringido. Dicho registro incluye, por lo menos, los siguientes datos: - Área donde estaba instalado el equipo. - Número o identificación de activo que el equipo de cómputo tenía asignado. - Nombre y firma de la persona que realiza el proceso de preparación final. - Fecha y hora en la que se realiza dicho proceso, tanto la de inicio como la de finalización. - Características del equipo (marca, modelo y número de serie) así como de los componentes de hardware al interior del equipo (marca y cantidad de la memoria volátil; marca, modelo y capacidad de los medios de almacenamiento no volátil; y demás componentes relevantes) en el momento de su recepción. - El destino que se le dará al equipo dado de baja. - Fecha en la que el equipo es efectivamente dado de baja.

vi. El formulario en el que se registran los incidentes contiene la siguiente información: - Registro del incidente donde se especifica: su tipo, gravedad, impacto, persona que lo detectó y personal que fue notificado. - Los procedimientos

implementados para la recuperación de los datos o aquellos procesos que permiten la pronta restauración de la operación del sistema. - Seguimiento donde se indique el personal que interviene en la atención del incidente, la metodología aplicada, los datos recuperados, y en su caso, aquellos datos que ha sido necesario grabar manualmente en el proceso de recuperación.

2. **Divulgación de incidentes**
    a. En caso de presentarse un incidente, se llevan a cabo las siguientes actividades:
        i. El responsable del personal de vigilancia emite un informe al Responsable de los SDP's a no más de 3 días naturales de haber ocurrido el incidente.
        ii. En caso de robo o extravío de datos personales en soportes físicos, el Director General, los titulares de las áreas administrativas del INCAR o el Responsable de los SDP's, al tener conocimiento del incidente, da vista al Órgano Interno de Control, al área jurídica y/o al servidor público que tenga facultades para presentar denuncias o querellas de cada dependencia o entidad, en términos del Estatuto Orgánico, según corresponda, para que cada uno, en el ámbito de sus atribuciones, determine lo conducente.

iii. En caso de robo o extravío de datos personales, se alerta a los titulares de los datos afectados para que tomen sus precauciones ante el posible uso ilegal de su identidad. Para tal efecto, el Responsable de los SDP's da aviso por escrito a dichos titulares, a más tardar cinco días naturales de haber ocurrido el incidente, recabando el acuse de recibo de esta notificación. Con anticipación a dicho escrito, si se cuentan con los datos actualizados, se da aviso por correo electrónico o por teléfono.

3. **Supervisión** El Comité de Información del INCAR propone la realización de una supervisión interna para las unidades administrativas que mantienen y operan SDP's así como a los terceros contratados.
4. **Equipo no autorizado**
    a. **Computadoras portátiles**
        i. No está permitido el libre acceso de computadoras portátiles a las zonas de acceso restringido de los SDP's.
        ii. Es posible autorizar el acceso temporal de computadoras portátiles siguiendo las recomendaciones descritas en el inciso "Operación cotidiana, Registro de actividades e inventario".
        iii. En caso de que se autorice el acceso temporal de una computadora portátil, el área de sistemas o el personal de vigilancia lleva a acabo una revisión inicial del equipo. Dicha revisión incluye:

- La revisión y el registro de la estructura de los medios de almacenamiento no volátil, específicamente el número de particiones y el espacio libre. - La detección de cualquier software que suponga un riesgo, ya sea por la perdida de datos personales o por la sustracción, como malware y herramientas de intrusión. - La inhabilitación de dispositivos de conexión inalámbrica que pudieran suponer un riesgo de extracción de datos personales por una persona que se encuentre fuera de las zonas de acceso restringido.

iv. Al finalizar la visita, se llevará a cabo una revisión final de la computadora portátil por parte del área de sistemas o del personal de vigilancia. Dicha revisión incluye:

1. La revisión y el registro de la estructura de los medios de almacenamiento no volátil a fin de comprobar que el número de particiones y el espacio libre sigue siendo el mismo que en la revisión inicial, lo que permite detectar si hay archivos almacenados en el equipo portátil que no estaban al inicio.
2. Las áreas no utilizadas (vacías) en los medios de almacenamiento no volátil se sobrescriben con un solo valor (unos o ceros) utilizando una herramienta especializada para ello.

b. **Dispositivos de almacenamiento externo**

i. Sin excepción alguna, no se permite el acceso de ningún tipo de dispositivo de almacenamiento externo ajeno a la institución o sin autorización.

ii. Es posible autorizar el acceso temporal de dispositivos de almacenamiento externo siguiendo las recomendaciones descritas en el apartado “Operación cotidiana” de la sección “Registro de actividades e inventario”.

iii. En caso de que se autorice el acceso temporal de dispositivos de almacenamiento externo, el área de sistemas o el personal de vigilancia lleva a acabo una revisión inicial del equipo. Dicha revisión incluye: **-** La revisión y el registro de la estructura de los medios de almacenamiento no volátil, específicamente el número de particiones y el espacio libre. **-** La detección de cualquier software que suponga un riesgo, ya sea por la perdida de datos personales o por la sustracción, como malware y herramientas de intrusión.

iv. Al finalizar la visita, se llevará a cabo una revisión final de los dispositivos de almacenamiento externo por parte del área de sistemas o del personal de vigilancia. Dicha revisión incluye: - La revisión y el registro de la estructura de los medios de almacenamiento no volátil a fin de comprobar que el número de particiones y el espacio libre sigue siendo el mismo que en la revisión inicial, lo que permitiría detectar si hay

archivos almacenados en el equipo portátil que no estaba al inicio.

c. **Otros dispositivos no autorizados**

i. En la medida de lo posible, no se permite el acceso de ningún tipo de dispositivo de almacenamiento externo portátil (memoria USB portátil, reproductor MP3, teléfono celular) ajeno a la institución. **2.** Es posible autorizar el acceso temporal de estos dispositivos siguiendo las recomendaciones descritas. **3.** Por el riesgo que implica, está prohibido el uso de dispositivos no autorizados para la transmisión de datos personales en soportes electrónicos, mediante traslado físico, sin antes haber sometido dichos datos personales a un proceso de preparación previa tal como se describe. **4.** Está prohibido introducir objetos que pudiesen dañar o alterar los soportes físicos y electrónicos que contengan datos personales tales como: tijeras, navajas, marcadores, alimentos o líquidos, entre otros.

12. MS para asegurar continuidad y enfrentar desastres

a. **Respaldo y recuperación de sistemas de datos personales automatizados**

i. **Medios de almacenamiento autorizados y no autorizados**

1. Los medios de almacenamiento no volátil autorizados para la generación y almacenamiento de copias de seguridad (o respaldos) se dividen en dos grupos: fijos y removibles. Los medios fijos son los discos duros internos. Los medios removibles, pueden ser (i) magnéticos (cintas, discos duros

externos), (ii) ópticos (CD's, DVD's) o (iii) magneto-ópticos (discos magneto-ópticos).

2. Los medios de almacenamiento no volátil autorizados se utilizan solos o en combinación, según las necesidades de respaldo y de restauración para garantizar la operación continúa del SDP.
3. El uso de las unidades para lectura y escritura de dichos medios autorizados es exclusivo para el personal de sistemas, quien se encarga de generar las copias de seguridad. Ello implica que, si se trata de unidades internas (dentro del gabinete de la computadora), existe cuando menos una forma de restringir su uso. Por otro lado, si se trata de unidades externas que se conectan a un puerto de comunicaciones, entonces existe cuando menos una forma de restringir el uso de dicho puerto.
4. Todos aquellos medios de almacenamiento así como sus respectivas unidades para lectura y escritura que no entren dentro de las descripciones anteriores son considerados *no autorizados*. Esto incluye los dispositivos portátiles que cuenten con memoria no volátil integrada y algún dispositivo de comunicación (por cable o inalámbrica) que permita el intercambio de datos con una computadora, por ejemplo: “memory-sticks”, las agendas digitales, los teléfonos celulares inteligentes, las cámaras digitales de instantáneas fijas o vídeo y los dispositivos portátiles para reproducción de música / vídeo como el Apple iPod y similares.
5. El encargado de los SDP’s, en colaboración con el personal de seguridad, ha implementado medidas para restringir el acceso y el uso de los dispositivos no autorizados. Los puntos de revisión y los sistemas de vídeo-vigilancia remoto coadyuvan a este propósito.

ii. **Inventario y clasificación de medios**

1. Existe un inventario de los equipos autorizados para almacenar información crítica así como de aquellos que se utilizan para generar copias de seguridad (respaldos) de la información.
2. Los medios de almacenamiento no volátil que contienen las copias de seguridad mencionadas son clasificados y protegidos por el área de sistemas o el personal de vigilancia a fin de evitar su extravío, robo o daño accidental.
3. Se siguen los procedimientos archivísticos necesarios y suficientes para clasificar los medios de almacenamiento no volátil, ya sean magnéticos, ópticos o magnetoópticos, dependiendo de las tecnologías utilizadas; en caso de que existan dos o más tecnologías, se lleva un control por cada una. El propósito es reducir el tiempo de espera para localizar los archivos que sea necesario restaurar.

iii. **Almacenamiento de respaldos**

1. El almacenamiento de los respaldos (es decir, de los medios de almacenamiento removibles que los contienen) se realiza en lugares seguros.
    a. El reemplazo de dichos medios de almacenamiento se lleva a cabo mediante un esquema calendarizado. Por ejemplo, un esquema de reemplazo mínimo incluye realizar un respaldo general cada 7 días, mismo que se almacena durante un mes, antes de reemplazarlo.
    b. Los respaldos se llevan a cabo a diario, en modo incremental y en línea, en caso de que el sistema lo permita. El séptimo día se realiza un respaldo general, fuera de línea, el cual es llevado, como lo menciona el punto anterior, a un lugar seguro para su resguardo.

c. Se lleva registro de las veces que un respaldo se introduce en, o se extrae de las áreas. Son sólo dos personas son las que estén autorizadas para realizar dichos trámites.

b. **Operación continua de sistemas de datos personales automatizados**

i. **Sitios alternos**

1. Existe un sitio alterno para restablecer la operación de un SDP automatizado, en el menor tiempo. Para ello, se tiene establecido un **Sitio alterno *frío*.** En este tipo de sitios alternos no se incluye ningún equipo de cómputo ni otros recursos, de no ser por un ambiente mínimo de operación que incluya aire acondicionado, corriente eléctrica, enlaces de comunicaciones, piso falso, etc. Este tipo de sitios alternos es el menos costoso y a la vez el que más demora supone para restaurar las operaciones de un SDP automatizado.
2. Dependiendo de la criticidad de un SDP automatizado, el Manual de Operaciones tiene definido el tiempo requerido para su restauración como sigue: (i) no esencial, se restaura en 30 días naturales, (ii) normal, en 7 días naturales, (iii) importante, en 72 hrs., (iv) urgente, en 24 hrs., (v) crítica o esencial, de 1 a 4 horas. Estos tiempos dan pauta para elegir el sitio alterno a utilizar.

ii. **Tecnologías de información y telecomunicaciones**

1. Existe un Plan de contingencia que documenta los procedimientos para restablecer la operación de los sistemas de redes en un sitio alterno que está separado del centro principal, fuera de las instalaciones del INCAR, en otra ciudad, a kilómetros de distancia.

2. A fin de tener identificados los mínimos requeridos para continuar con la operación, dicho Plan de contingencia está basado en: (i) un análisis realizado para determinar los requerimientos de soporte de una red, como serían los requerimientos de equipo, periféricos, cableado, etc.; y (ii) un análisis para identificar el tipo de comunicaciones, como serían los enlaces requeridos, líneas telefónicas y servicios de redes de comunicación electrónica, tanto de área local como de área ampliada.

iii. **Personal para emergencias**

1. Existe un Plan de contingencia que identifica al personal que lleva la operación de un SDP automatizado y que cuenta con la capacitación requerida para seguir los procedimientos de restauración en caso de desastre.
2. Dichas personas estuvieron involucradas en la creación de la documentación necesaria para el mencionado plan.
3. Dicho Plan de contingencia designa el personal de cada área necesario para efectuar la operación y administración de los SDP's automatizados que se restauran en el sitio alterno.

c. **Registro de actividades**

i. **Pruebas y simulacros**

1. El Responsable de los SDP's, en coordinación con el área de sistemas y el personal de vigilancia, lleva a cabo pruebas y simulacros para minimizar riesgos en caso de presentarse alguna eventualidad adversa y para comprobar que los sistemas de seguridad y prevención funcionan correctamente y en el tiempo estimado como óptimo. Estas tareas se llevan a cabo periódicamente, según el nivel de criticidad de la información.

2. Existe un registro de pruebas y simulacros que contiene, cuando menos, los siguientes datos: - Fecha y hora, tanto de inicio como de finalización. - Encargado de realizarlas. - Encargado de evaluarlas. - Tiempo de restauración. - Firma (visto bueno) de los Responsables. - Observaciones. - Sugerencias de mejora. El propósito de este registro es permitir su análisis y evaluación a fin de realizar las adecuaciones necesarias antes de que se presente una contingencia.

ii. **Divulgación de incidentes**

1. En caso de que el incidente se refiera a la pérdida de información debida a fallas en el equipo o en sus dispositivos de almacenamiento, ya sea por fallas en instalaciones, acontecimientos de casos fortuitos o de fuerza mayor (desastres naturales, incendios, huelgas, etc.), entonces procede la declaración de este. En ese momento, se pone en marcha el Plan de Continuidad del Negocio, para asegurar la continuidad de la operación o el Plan de Recuperación en caso de desastres para enfrentar el incidente. Cuando menos existe uno de estos planes en el INCAR.
2. En caso de que el incidente se refiera a actos deliberados (alteración, pérdida o robo de datos personales), se sigue el procedimiento que esa dependencia o entidad tenga definido. En caso de que dicho procedimiento no lo incluya, además, se llevan a cabo las siguientes actividades, sin necesidad de que se realicen en el orden que aparecen:
    a. El responsable del personal de vigilancia emite un informe al Responsable de los SDP’s a no más de 3 días naturales de haber ocurrido el incidente.

b. En caso de robo o extravío de datos personales en soportes electrónicos, el Director General, los titulares de las áreas administrativas del INCAR o el Responsable de los SDP's, al tener conocimiento del incidente, da vista al Órgano Interno de Control, al área jurídica y/o al servidor público que tenga facultades para presentar denuncias o querellas de cada dependencia o entidad, en términos del Estatuto Orgánico, según corresponda, para que cada uno, en el ámbito de sus atribuciones, determine lo conducente.

c. En caso de robo o extravío de datos personales, se alerta a los titulares de los datos afectados para que tomen sus precauciones ante el posible uso ilegal de su información. Para tal efecto, el Responsable de los SDP's da aviso por escrito a dichos titulares, a más tardar cinco días naturales de haber ocurrido el incidente, recabando el acuse de recibo de esta notificación. Con anticipación a dicho escrito, si se cuentan con los datos actualizados, se da aviso por correo electrónico o por teléfono.

iii. **Supervisión** El Comité de información del INCAR propone la realización de una supervisión interna a las unidades administrativas que mantienen y operan SDP's así como a los terceros contratados.

d. **Documentación de MS en procesos y políticas del SDP**

i. **Manual de operaciones** Existe un Manual de operaciones donde están documentados los procesos y procedimientos que los servidores públicos llevan a cabo dentro del INCAR. Aquellos procesos y procedimientos en los que se describe la forma en que los titulares de los datos y los servidores públicos (usuarios, personal autorizado,

encargados, responsables) interactúan con los SDP's, incorporan la adopción de estos MS recomendados para la protección de datos personales.

e. **Sensibilización y capacitación**

i. Se sensibilizará a través de la difusión de los materiales sobre protección de datos personales en soportes físicos y soportes electrónicos al interior del INCAR y de ser posible se implementará un curso.

ii. Esta sensibilización será permanente y de ser posible, se implementará un curso al menos una vez cada año, llevando un registro.

iii. El objetivo de la sensibilización será el de dar a conocer la relevancia de la seguridad de datos personales y sus responsabilidades mediante firma autógrafa que se recaba en una lista que archiva el responsable de los SDP's en las áreas administrativas del INCAR.

iv. Se sensibiliza a proveedores externos que interactúan con uno o más SDP's y a quienes también se exige aseguren la protección de datos personales.

f. **Cartas compromiso, cláusulas y contratos de confidencialidad**

i. Al menos cada dos años, el Responsable de los SDP's recibe (y archiva) una carta compromiso de parte de cada uno de los miembros del personal autorizado que interactúa con uno o más SDP's.

ii. En dicha carta, el servidor público manifiesta, con su firma autógrafa, su compromiso para realizar su trabajo apegándose a los MS que apliquen a los SDP's y manifiesta conocer el marco jurídico a fin de garantizar la custodia.

iii. El INCAR cuenta con un contrato de confidencialidad que ha firmado con cada proveedor o prestador de servicios que llama para la realización de servicios que impliquen interactuar con los SDP's.

ANEXO 3 Medidas adicionales mínimas aplicables al nivel medio de seguridad

Los sistemas de datos personales que contengan alguno de los datos que se enlistan a continuación, además de cumplir con las medidas de seguridad de nivel básico, deberán observar las marcadas con nivel medio.

1. **MS aplicables al Nivel medio**
    a. Los sistemas de datos personales que contengan alguno de los datos que se enlistan a continuación, además de cumplir con las medidas de seguridad de nivel básico, deberán observar las marcadas con nivel medio.
        i. **Datos Patrimoniales**: Bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos y egresos, cuentas bancarias, seguros, afores, fianzas, servicios contratados, referencias personales, entre otros.
        ii. **Datos sobre procedimientos administrativos seguidos en forma de juicio y/o jurisdiccionales:** Información relativa a una persona que se encuentre sujeta a un procedimiento administrativo seguido en forma de juicio o jurisdiccional en materia laboral, civil, penal o administrativa.
        iii. **Datos Académicos:** Trayectoria educativa, títulos, cédula profesional, certificados y reconocimientos, entre otros.
        iv. **Transito y movimientos migratorios:** Información relativa al transito de las personas dentro y fuera del país e información migratoria de las personas, entre otros.
    b. **Recomendaciones**
        i. **MS para datos personales en soportes físicos**
            1. **Área de recepción de datos personales**
                a. Cualquier persona puede identificar con facilidad al personal autorizado que labora en el área de recepción gracias a que los nombres completos y

fotografías de dicho personal se exhiben en un lugar visible dentro y fuera de dicha área.

b. El Encargado de los SDP's actualiza los nombres completos y fotografías que se exhiben en el área de recepción conforme se van presentando cambios de personal.

c. No está permitido el libre acceso y el uso de aquellos aparatos referidos en la sección "Equipo no autorizado" de los Lineamientos del IFAI y las que sean establecidas por el área de Informática del INCAR dentro del área de recepción.

2. **Área de resguardo de datos personales**

a. De existir ventanas o muros divisorios transparentes en el área de resguardo, la visión está obstruida mediante una película translúcida (papel albanene, por ejemplo).

b. El mobiliario utilizado para almacenar los datos personales en soportes físicos cuenta con cerraduras, dispositivos electrónicos o cualquier otra tecnología que impida la libre apertura de sus puertas, cajones o compartimientos. Tales mecanismos quedan cerrados en horas no hábiles.

c. Cualquier persona puede identificar con facilidad al personal autorizado que labora en el área de resguardo gracias a que los nombres completos y fotografías de dicho personal se exhiben en un lugar visible dentro y fuera de dicha área.

d. El Encargado de los SDP's actualiza los nombres completos y fotografías que se exhiben en el área de resguardo conforme se presentan cambios de personal.

e. No está permitido el libre acceso y el uso de aquellos aparatos referidos en la sección "Equipo no autorizado" dentro del área de resguardo.

3. **Área de consulta de datos personales**
    a. De existir ventanas o muros divisorios transparentes, la visión está obstruida mediante una película translúcida (papel albanene, por ejemplo).
    b. La puerta de acceso del área de consulta cuenta con cerradura, dispositivo electrónico o cualquier otra tecnología que impida su libre apertura. Este mecanismo queda cerrado en horas no hábiles o cuando el personal autorizado que ahí labora abandona el área.
    c. Cualquier persona puede identificar con facilidad al personal autorizado que labora en el área de consulta gracias a que los nombres completos y fotografías de dicho personal se exhiben en un lugar visible dentro y fuera de dicha área.
    d. El Encargado de los SDP's actualiza los nombres completos y fotografías que se exhiben en el área de consulta conforme se presentan cambios de personal.
    e. No está permitido el libre acceso y el uso de aquellos aparatos referidos en la sección "Equipo no autorizado" de los Lineamientos del IFAI y las que sean establecidas por el área de Informática del INCAR dentro del área de consulta.
4. **Acceso y consulta de datos personales**
    a. **Acceso**
        i. El personal que tienen intención de ingresar a una zona de acceso restringido se registra y entrega una identificación oficial con fotografía (credencial de elector, pasaporte, etc.) al personal de vigilancia que atiende dicho punto de revisión.
        ii. En todo caso, la dependencia o entidad adopta las medidas de seguridad necesarias para el ingreso a una zona de acceso restringido.
    b. **Personas autorizadas y no autorizadas** Cada acceso y consulta realizada por personas no autorizadas es considerada como un incidente

de intrusión que se denuncia ante las autoridades competentes para su investigación.

c. **Medidas para la prevención de intrusiones** Además, el personal de vigilancia realiza funciones de forma permanente en las zonas de acceso restringido de los SDP's.

5. **Registro de actividades**

a. **Operación cotidiana**

i. El Responsable de los SDP's mantiene estricto control y registro de: a) Las autorizaciones emitidas a los usuarios que solicitan permiso para extraer datos personales en soportes físicos del área de consulta. Para ello, el Encargado anota - Por qué necesita llevárselos - Las autorizaciones emitidas a los usuarios que solicitan permiso para introducir a las zonas de acceso restringido aparatos tales como los mencionados en la sección "Equipo no autorizado". Para ello, el Encargado anota: - Por qué necesita introducirlo

b. **Divulgación de incidentes** A no más de 3 días naturales de haber ocurrido el incidente, el Responsable de los SDP's da aviso al público mediante un desplegado de prensa que difunde el hecho por diversos medios, según la gravedad del caso, a escala local, regional o nacional.

c. **Baja de datos personales** Para proceder a la baja documental de soportes físicos que contienen datos personales, deberán observarse las disposiciones establecidas por el Capítulo III De la Conservación de Archivos, de los Lineamientos Generales para la organización y conservación de los archivos de las dependencias y entidades de la Administración Pública Federal (D.O.F 20/02/04), y además:

i. **1.** El Encargado de los SDP's:

1. Sigue procedimientos y utiliza mecanismos para asegurar la valoración y en su caso, destrucción de soportes físicos que contienen datos personales.

2. Si se realizan la separación de materiales para su reciclaje (como podría suceder con el papel, el cartón, el metal y el plástico), los datos personales contenidos en materiales reciclables son triturados y la viruta resultante se entrega directamente a una empresa que los recibe para procesarlos de inmediato, garantizando por escrito que no serán examinados para su eventual reconstrucción.

6. **MS para datos personales en soportes electrónicos**
   a. **Área de recepción de datos personales**
      i. Dicho equipo de cómputo está provisto de la tecnología necesaria y suficiente para verificar la identidad del personal autorizado que labora en el área de recepción. Ello implica que, mediante la verificación de claves de acceso, dicho personal accede al equipo a fin de realizar el tratamiento que corresponda a la recepción de datos personales.
      ii. Cualquier persona puede identificar con facilidad al personal autorizado que labora en el área de recepción gracias a que los nombres completos y fotografías de dicho personal se exhiben en un lugar visible dentro y fuera de dicha área. [Nivel medio]
      iii. El Encargado de los SDP's actualiza los nombres completos y fotografías que se exhiben en el área de recepción conforme se van presentando cambios de personal.
      iv. No está permitido el libre acceso y el uso de aquellos aparatos referidos en la sección "Equipo no autorizado" de los Lineamientos del IFAI y las que sean establecidas por el área de Informática del INCAR dentro del área de recepción.

7. **Área de resguardo de datos personales**
   a. De existir ventanas o muros divisorios transparentes, la visión está obstruida mediante una película translúcida (papel albanene, por ejemplo).

b. Dicho equipo de cómputo está provisto de la tecnología necesaria y suficiente para verificar la identidad del usuario que labora en el área de resguardo. Ello implica que, mediante la verificación de claves de acceso, dicho personal accede al equipo a fin de realizar el tratamiento que corresponda al resguardo de datos personales.
c. Cualquier persona puede identificar con facilidad al personal autorizado que labora en el área de resguardo gracias a que los nombres completos y fotografías de dicho personal se exhiben en un lugar visible dentro y fuera de dicha área.
d. El Encargado de los SDP's actualiza los nombres completos y fotografías que se exhiben en el área de resguardo conforme se presentan cambios de personal.

8. **Área de consulta de datos personales**
   a. De existir ventanas o muros divisorios transparentes en el área de consulta, la visión está obstruida mediante una película translúcida (papel albanene, por ejemplo).
   b. La puerta de acceso del área de consulta cuenta con cerradura, dispositivo electrónico o cualquier otra tecnología que impida su libre apertura. Este mecanismo queda cerrado en horas no hábiles o cuando el personal autorizado que ahí labora abandona el área.
   c. Dicho equipo de cómputo está provisto de la tecnología necesaria y suficiente para verificar la identidad del usuario que labora en el área de consulta. Ello implica que, mediante la verificación de claves de acceso, dicho personal accede al equipo a fin de realizar el tratamiento que corresponda al resguardo de datos personales.
   d. Cualquier persona puede identificar con facilidad al personal autorizado que labora en el área de consulta gracias a que los nombres completos y fotografías de dicho personal se exhiben en un lugar visible dentro y fuera de dicha área.

e. El Encargado de los SDP's actualiza los nombres completos y fotografías que se exhiben en el área de consulta conforme se presentan cambios de personal.

f. No está permitido el libre acceso y el uso de aquellos aparatos referidos en la sección "Equipo no autorizado" dentro del área de consulta.

9. **Acceso y consulta de datos personales**

   a. **Acceso**

      i. El personal que tienen intención de ingresar a una zona de acceso restringido se registra y entrega una identificación oficial con fotografía (credencial de elector, pasaporte, etc.) al personal de vigilancia que atiende dicho punto de revisión.

      ii. En todo caso, la dependencia o entidad adopta las medidas de seguridad necesarias para el ingreso a una zona de acceso restringido.

   b. **Consulta**

      i. El usuario consulta los datos personales en soportes electrónicos dentro del área de consulta.

10. **Medidas para la prevención de intrusiones**

   a. Además, el personal de vigilancia realiza funciones de forma permanente en las zonas de acceso restringido de los SDP's.

   b. Dicho equipo de cómputo está provisto de la tecnología necesaria y suficiente para verificar la identidad del usuario que labora en estas zonas y que utiliza tal equipo. Ello implica que, mediante la verificación de claves de acceso, dicho usuario accede al equipo para interactuar con el o los SDP's que tiene autorizados.

11. **Registro de actividades**

   a. **Operación cotidiana**

      i. El Responsable de los SDP's mantiene estricto control y registro de:

      - Las autorizaciones emitidas a los usuarios que solicitan permiso

para extraer datos personales en soportes electrónicos del área de consulta. Para ello, el Encargado anota: - Por qué necesita llevárselos. - Las autorizaciones emitidas a los usuarios que solicitan permiso para introducir a las zonas de acceso restringido aparatos tales como los mencionados en la sección “Equipo no autorizado” de los Lineamientos del IFAI y las que sean establecidas por el área de Informática del INCAR. Para ello, el Encargado anota: - Por qué necesita introducirlo.

b. **Divulgación de incidentes**

i. A no más de 3 días naturales de haber ocurrido el incidente, el Responsable de los SDP’s da aviso al público mediante un desplegado de prensa que difunde el hecho por diversos medios, según la gravedad del caso, a escala local, regional o nacional.

12. **MS para transmisión de datos personales**

a. **Transmisión de datos personales en soportes físicos**

i. **Transmisión mediante traslado físico**

1. La transmisión al exterior se realiza mediante un servicio de mensajería externo. En este caso, se define un destinatario primario y otro secundario por si el mensajero no encuentra al primero.
2. La entrega del paquete se realiza sólo si el destinatario acredita su identidad. Para ello, el destinatario presenta una identificación oficial con fotografía (credencial de elector, pasaporte, etc.) y el mensajero recaba nombre, firma y un número de referencia que aparezca en tal identificación además de la fecha de entrega.
3. El mensajero no entrega el paquete si el destinatario no puede acredita su identidad. En este caso, es imperativo que el mensajero regrese dicho paquete al transmisor.

4. El Responsable de los SDP's verifica que el mensajero entregó el paquete al destinatario. Si el transmisor detecta que dicho paquete fue entregado a otra persona, da inicio al proceso de atención de un incidente.

b. **Transmisión de datos personales en soportes electrónicos**

i. **Preparación previa a la transmisión**

1. Los datos personales que son enviados a un destinatario autorizado para manipularlos o procesarlos son sometidos a un proceso de preparación previa a la transmisión. En este caso, el encargado que realiza dicho proceso: Somete dichos archivos a un proceso de encriptación que los proteja durante su trayecto aplicando un nivel de encriptación ALTO, no menor a 1024 bits.
2. Los datos personales que son enviados a un destinatario No autorizado para manipularlos o procesarlos son sometidos a un proceso distinto de preparación previa a la transmisión. En este caso, el encargado que realiza dicho proceso:
3. Genera archivos electrónicos que contengan los datos personales solicitados en un formato protegido, de manera que el destinatario pueda examinar su contenido pero no pueda editarlo, copiarlo ni imprimirlo, en la medida de lo posible por los avances técnicos existentes.
4. Somete los archivos resultantes a un proceso de encriptación que proteja los archivos durante su trayecto aplicando un nivel de encriptación MEDIO, no menor a 512 bits.

ii. **Transmisión mediante traslado físico**

1. La transmisión al exterior se realiza mediante un servicio de mensajería externo. En este caso, se define un destinatario

primario y otro secundario por si el mensajero no encuentra al primero.

2. La entrega del paquete se realiza sólo si el destinatario acredita su identidad. Para ello, el destinatario presenta una identificación oficial con fotografía (credencial de elector, pasaporte, etc.) y el mensajero recaba nombre, firma y un número de referencia que aparezca en tal identificación además de la fecha de entrega. [Nivel medio]
3. El mensajero no entrega el paquete si el destinatario no puede acredita su identidad. En este caso, es imperativo que el mensajero regrese dicho paquete al transmisor.
4. El Encargado de los SDP's verifica que el mensajero entregó el paquete al destinatario. Si el transmisor detecta que dicho paquete fue entregado a otra persona, da inicio al proceso de atención de un incidente.

iii. **Transmisión mediante redes de comunicación electrónica** El transmisor recaba por escrito acuse de recibo del destinatario, ya sea por correo electrónico o mediante oficio enviado por fax.

iv. **Medidas para la prevención de intrusiones desde el exterior**

1. Se aplican las medidas necesarias y suficientes para que los puntos de acceso inalámbrico a la red de comunicación electrónica de la dependencia o entidad sean seguros y no existan huecos que puedan ser aprovechados por intrusos.
2. Las recomendaciones presentadas en la sección "4. MS para equipo de cómputo en zonas de acceso restringido" aplican en esta sección. [Nivel medio]
3. El personal de sistemas mantiene actualizada la memoria técnica de la red de comunicación electrónica con el fin de identificar los equipos inicialmente configurados y puestos a

disposición del personal autorizado para interactuar los SDP's.

4. Si un equipo de cómputo queda en manos de una persona no autorizada o si es dado de baja, se utiliza la memoria técnica mencionada para cancelar la configuración del equipo en cuestión.
5. El personal de vigilancia o el Encargado de los SDP's, en coordinación con el área de sistemas, realiza de manera periódica y en forma programada análisis de vulnerabilidades y pruebas de intrusión controladas en la infraestructura de cómputo, almacenamiento y comunicaciones. El propósito de esta actividad es aplicar las medidas correctivas necesarias a fin de cerrar las vulnerabilidades encontradas y así evitar posibles incidentes de intrusión

13. **Registro de actividades**
    a. **Operación cotidiana**
        i. El Encargado de los SDP's mantiene estricto control y registro.
    b. **Divulgación de incidentes**
        i. A no más de 3 días naturales de haber ocurrido el incidente, el Responsable de los SDP's da aviso al público mediante un desplegado de prensa que difunde el hecho por diversos medios, según la gravedad del caso, a escala local, regional o nacional.
14. **MS para equipo de cómputo en zonas de acceso restringido**
    a. **Computadoras de escritorio**
        i. **Recepción**
            1. El proceso de preparación inicial de la computadora de escritorio incluye, antes de instalar el software, sobrescribir con un solo valor (unos o ceros) el 100% del medio principal

de almacenamiento no volátil con alguna herramienta especializada para ello.

2. La lista de software autorizado para computadoras de escritorio en sitios de acceso restringido es un documento que prepara y actualiza el área de sistemas de la dependencia o entidad. Este documento se prepara en coordinación con el Responsable de los SDP's, según las necesidades y las funciones que desempeña el personal autorizado a su cargo.
3. Las únicas personas autorizadas para realizar el proceso de preparación inicial son miembros del personal de las áreas de sistemas o de vigilancia.

ii. **Operación**

1. Están deshabilitados (en el interior del equipo) o cancelados (en el exterior) los puertos de comunicación (USB, paralelo, serial, etc.) que no se utilizan. Los cables o dispositivos conectados a los puertos que sí se utilizan están asegurados para evitar su desconexión. Las cancelaciones pueden ser abiertas por personal autorizado del área de sistemas.
2. Están deshabilitados (en el interior del equipo) o cancelados (en el exterior) los dispositivos de almacenamiento removible (unidades de disco flexible, quemadores de CD/DVD, etc.). Las cancelaciones pueden ser abiertas por personal de sistemas.
3. No existen dispositivos de conexión inalámbrica (Wi-Fi, Bluetooth, infrarrojo, etc,) en las computadoras de escritorio asignadas dentro de las zonas de acceso restringido de los SDP's.

15. **Impresoras y otros equipos periféricos autorizados**

a. **Recepción**

i. Las impresoras y los equipos periféricos autorizados (monitores, pantallas planas, etc.) usados en las zonas de acceso restringido de un SDP, sean nuevos o usados, pasan por un proceso de preparación inicial. Con ello se busca la presencia de puertos de comunicación (USB, paralelo, red local, por ejemplo) adicionales al principal que pudieran utilizarse para conectar dispositivos como los descritos en la sección “Equipo no autorizado”.

ii. Los puertos adicionales antes mencionados quedan inhabilitados (en el interior del equipo) o cancelados (en el exterior), mientras que los cables conectados a los puertos principales quedan asegurados para evitar su desconexión. Las cancelaciones pueden ser abiertas por el personal autorizado del área de sistemas. [Nivel medio]

iii. Las únicas personas autorizadas para realizar el proceso de preparación inicial son miembros del personal de sistemas y de vigilancia.

iv. El Encargado de los SDP’s supervisa y verifica que el equipo de cómputo cumpla con los requerimientos de instalación establecidos y las configuraciones de seguridad definidas.

v. El proceso de preparación inicial de una impresora o de un equipo periférico autorizado que se asigna en zonas de acceso restringido queda registrado en un formulario. Este documento es archivado por el área de sistemas o por el personal de vigilancia.

b. **Resguardo**

i. El equipo de impresión está asegurado físicamente para evitar el robo o la sustracción de cartuchos de tinta, piezas o partes. Para tal propósito, está resguardado mediante cajones de protección,

candados o cualquier otro dispositivo que impida la manipulación del equipo y el acceso físico al interior del equipo.

ii. El equipo de almacenamiento removible externo se mantiene bajo custodia del área de sistemas o del personal de vigilancia.

c. **Operación**

i. El uso de impresoras y equipo periférico autorizado que se conecta directamente a computadoras de escritorio y servidores dentro de zonas de acceso restringido es vigilado, supervisado o, en su caso, autorizado por el Responsable de los SDP's.

ii. Las únicas personas autorizadas para utilizar el equipo de almacenamiento removible externo son miembros del personal de sistemas y de vigilancia.

d. **Baja.**

i. Las impresoras y los equipos periféricos autorizados que en su interior contienen uno o más medios de almacenamiento no volátil, fijos o removibles, reciben atención especial. En este caso, el proceso de preparación final incluye transferir a otro equipo los archivos que contengan información que sea preciso conservar y sobrescribir con un solo valor (unos o ceros) el 100% de los medios de almacenamiento no volátil con alguna herramienta especializada para ello.

ii. Las únicas personas autorizadas para realizar el proceso de preparación final son miembros del personal de sistemas y de vigilancia.

16. **Registro de actividades e inventario**

a. **Operación cotidiana**

i. El formulario donde se asientan los detalles del proceso de preparación inicial que se lleva a cabo para cada impresora y cada equipo periférico autorizado asignado en áreas de acceso

restringido. Dicho registro incluye, por lo menos, los siguientes datos: **-** Área donde queda instalado el equipo. **2.** El formulario donde se asientan los resultados del proceso de preparación final que se lleva a cabo para cada impresora y cada equipo periférico autorizado asignado en áreas de acceso restringido. Dicho registro incluye: **-** Nombre y firma (visto bueno) del Responsable de los SDP's.

b. **Divulgación de incidentes** A no más de 3 días naturales de haber ocurrido el incidente, el Responsable de los SDP's da aviso al público mediante un desplegado de prensa que difunde el hecho por diversos medios, según la gravedad del caso, a escala local, regional o nacional.

17. **Equipo no autorizado**

a. **Computadoras portátiles**

i. En caso de que se autorice el acceso temporal de una computadora portátil, el área de sistemas o el personal de vigilancia lleva a acabo una revisión inicial del equipo. Dicha revisión incluye: - La inhabilitación de dispositivos de conexión inalámbrica que pudieran suponer un riesgo de extracción de datos personales por una persona que se encuentre fuera de las zonas de acceso restringido.

ii. En caso de ser necesario el traslado de datos personales al equipo no autorizado, éste sería con las siguientes restricciones: sólo lectura, no para modificación, no para sustracción, no para impresión, no para quemado.

iii. Por el riesgo que implica, está prohibido el uso de computadoras portátiles para la transmisión de datos personales en soportes electrónicos, mediante traslado físico, sin antes haber sometido dichos datos personales a un proceso de preparación previa tal como se describe en la sección "3. MS para transmisión de datos personales".

b. **Dispositivos de almacenamiento externo**

i. En caso de que se autorice el acceso temporal de dispositivos de almacenamiento externo, el área de sistemas o el personal de vigilancia lleva a acabo una revisión inicial del equipo. Dicha revisión incluye: **-** La inhabilitación de dispositivos de conexión inalámbrica que pudieran suponer un riesgo de extracción de datos personales por una persona que se encuentre fuera de las zonas de acceso restringido.

ii. En caso de ser necesario el traslado de datos personales al equipo no autorizado, éste sería con las siguientes restricciones: sólo lectura, no para modificación, no para sustracción, no para impresión, no para quemado.

iii. Al finalizar la visita, se llevará a cabo una revisión final de los dispositivos de almacenamiento externo por parte del área de sistemas o del personal de vigilancia. Dicha revisión incluye: **-** Las áreas no utilizadas (vacías) en los medios de almacenamiento no volátil se sobrescriben con un solo valor (unos o ceros) utilizando una herramienta especializada para ello.

iv. Por el riesgo que implica, está terminantemente prohibido el uso de dispositivos de almacenamiento externo para la transmisión de datos personales en soportes electrónicos, mediante traslado físico, sin antes haber sometido dichos datos personales a un proceso de preparación previa tal como se describe en la sección “3. MS para transmisión de datos personales”. MS para asegurar continuidad y enfrentar desastres

18. **Respaldo y recuperación de sistemas de datos personales automatizados**

a. **Almacenamiento de respaldos**

CONTROL DE EMISIÓN			
	Elaboró :	**Revisó :**	**Autorizó**:
Nombre			
Firma			
Fecha			

i. El almacenamiento de los respaldos (es decir, de los medios de almacenamiento removibles que los contienen) se realiza en lugares seguros, preferentemente en bóvedas de seguridad.

ii. El reemplazo de dichos medios de almacenamiento se lleva a cabo mediante un esquema calendarizado. Por ejemplo, un esquema de reemplazo mínimo incluye realizar un respaldo general cada 7 días, mismo que se almacena durante un mes, antes de reemplazarlo. En la bóveda, quedan siempre cuatro semanas de respaldo.

iii. Se lleva registro de las veces que un respaldo se introduce en, o se extrae de, las bóvedas. Son sólo dos (y cuando mucho tres) personas las que estén autorizadas para realizar dichos tramites.

b. **Operación continua de sistemas de datos personales automatizados**

i. **Sitios alternos** Existe un sitio alterno para restablecer la operación de un SDP automatizado, en el menor tiempo posible, en caso de un desastre. Para ello, se tiene establecido un **Sitio alterno *frío*.** En este tipo de sitios alternos no se incluye ningún equipo de cómputo ni otros recursos, de no ser por un ambiente mínimo de operación que incluya aire acondicionado, corriente eléctrica, enlaces de comunicaciones, piso falso, etc. Este tipo de sitios alternos es el menos costoso y a la vez el que más demora supone para restaurar las operaciones de un SDP automatizado.

c. **Registro de actividades**

i. **Divulgación de incidentes** En caso de que dicho procedimiento no lo incluya, además, se llevan a cabo las siguientes actividades, sin necesidad de que se realicen en el orden que aparecen: A no más de 3 días naturales de haber ocurrido el incidente, el Responsable de los SDP's da aviso al público mediante un desplegado de prensa que difunde el hecho por diversos medios, según la gravedad del caso, a escala local, regional o nacional.

19. **Documentación de MS en procesos y políticas del SDP**

a. **Cartas compromiso, cláusulas y contratos de confidencialidad**

i. Al menos cada dos años, el Responsable de los SDP's recibe (y archiva) una carta compromiso de parte de cada uno de los miembros del personal autorizado que interactúa con uno o más SDP's.

ii. En dicha carta, el servidor público manifiesta, con su firma autógrafa, su compromiso para realizar su trabajo apegándose a los MS que apliquen a los SDP's en esa dependencia o entidad. Además, el servidor público manifiesta conocer los Lineamientos, el Reglamento y la Ley que integran el marco jurídico de las presentes Recomendaciones a fin de garantizar al ciudadano la custodia de sus datos personales.

ANEXO 4

Medidas adicionales mínimas aplicables al nivel alto de seguridad

Los sistemas de datos personales que contengan alguno de los datos que se enlistan a continuación, además de cumplir con las medidas de seguridad de nivel básico y medio, deberán observar las marcadas con nivel alto.

1. ***Datos Ideológicos:*** *Creencia religiosa, ideología, afiliación política y/o sindical, pertenencia a organizaciones de la sociedad civil y/o asociaciones religiosas, entre otros.*
2. **Datos de Salud:** Estado de salud, historial clínico, alergias, enfermedades, información relacionada con cuestiones de carácter psicológico y/o psiquiátrico, incapacidades médicas, intervenciones quirúrgicas, vacunas, consumo de sustancias tóxicas, uso de aparatos oftalmológicos, ortopédicos, auditivos, prótesis, entre otros.
3. **Características personales:** Tipo de sangre, ADN, huella digital, u otros análogos.
4. **Características físicas:** Color de piel, color de iris, color de cabello, señas particulares, estatura, peso, complexión, discapacidades, entre otros.
5. **Vida sexual:** Preferencia sexual, hábitos sexuales, entre otros.
6. **Origen:** Étnico y racial.

Acceso y consulta de datos personales

El usuario consulta los datos personales en soportes físicos dentro del área de consulta.

1. Medidas para la prevención de intrusiones

a. Las zonas de acceso restringido cuentan con un sistema remoto de vídeo-vigilancia que permite vigilar la puerta de acceso y el interior de dichas áreas. Dicho sistema cuenta con cámaras para visión nocturna, un sistema de grabación que opere las 24 horas, los 7 días de la semana (24x7) y un archivo que acumula grabaciones de los dos meses anteriores.

b. En caso de ocurrir un incidente de intrusión, el personal de vigilancia acude de inmediato a la zona de acceso restringido presuntamente violada para corroborar el hecho. De comprobarse este, la grabación realizada por el sistema de vídeo-vigilancia remota se transfiere a un soporte físico para que pueda ser utilizado como prueba por las autoridades que investiguen el caso.

c. **Registro de actividades**

i. **Operación cotidiana**

1. El sistema de vídeo-vigilancia remoto registra las actividades diarias así como los incidentes en las zonas de acceso restringido. [Nivel alto]

2. Medidas para la prevención de intrusiones

a. Las zonas de acceso restringido cuentan con un sistema de vídeo-vigilancia remota que permite vigilar la puerta de acceso y el interior de dichas áreas. Dicho sistema cuenta con cámaras para visión nocturna, un sistema de grabación que opere las 24 horas, los 7 días de la semana (24x7) y un archivo que acumula grabaciones de los dos meses anteriores. [Nivel alto]

b. En caso de ocurrir un incidente de intrusión, el personal de vigilancia acude de inmediato a la zona de acceso restringido presuntamente violada para corroborar el hecho. De comprobarse este, la grabación realizada por el sistema de vídeo-vigilancia remota se transfiere a un soporte físico para que pueda ser utilizado como prueba por las autoridades que investiguen el caso. [Nivel alto]

i. **Registro de actividades**

1. **Operación cotidiana**

a. El sistema remoto de vídeo-vigilancia registra las actividades diarias así como los incidentes en las zonas de acceso restringido.

3. MS para transmisión de datos personales

a. **Medidas para la prevención de intrusiones desde el exterior**

i. Existen dispositivos de alta seguridad instalados en caso de que la red de comunicación electrónica (que conecta los servidores que contienen los datos personales con las computadoras que se utilizan para acceder a ellos) esté conectada a Internet. Los dispositivos instalados incluyen sistemas de protección perimetral (cortafuegos), de detección de intrusos, filtros de contenido, de prevención de intrusiones y de análisis de protocolos.