GACETA DEL GOBIERNO

ESTADO DE MÉXICO

Periódico Oficial del Gobierno del Estado Libre y Soberano de México
REGISTRO DGC NUM. 001 1021 CARACTERISTICAS 113282801
Directora: Lic. Graciela González Hernández

Mariano Matamoros Sur No. 308 C.P. 50130
Tomo CXCV A:202/3/001/02
Número de ejemplares impresos: 400

Toluca de Lerdo, Méx., miércoles 8 de mayo de 2013
No. 86

SUMARIO:

"2013. Año del Bicentenario de los Sentimientos de la Nación"

SECCION TERCERA

INSTITUTO DE TRANSPARENCIA, ACCESO A LA INFORMACION PUBLICA Y PROTECCION DE DATOS PERSONALES DEL ESTADO DE MEXICO Y MUNICIPIOS

LINEAMIENTOS SOBRE MEDIDAS DE SEGURIDAD APLICABLES A LOS SISTEMAS DE DATOS PERSONALES QUE SE ENCUENTRAN EN POSESIÓN DE LOS SUJETOS OBLIGADOS DE LA LEY DE PROTECCIÓN DE DATOS PERSONALES DEL ESTADO DE MÉXICO, que expide el Pleno del Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de México y Municipios, con fundamento en lo dispuesto por el artículo 66, fracción IV, de la Ley de Protección de Datos Personales del Estado de México, al tenor de las siguientes:

CONSIDERACIONES

Que el Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de México y Municipios es la autoridad encargada de garantizar a toda persona la protección de sus datos personales que se encuentren en posesión de los Sujetos Obligados, a través de la aplicación de la Ley de Protección de Datos Personales del Estado de México.

Que son atribuciones del Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de México y Municipios establecer políticas y lineamientos para el manejo, tratamiento, seguridad y protección de los datos personales en posesión de los Sujetos Obligados; elaborar y actualizar el registro del nivel de seguridad aplicable a los sistemas de datos personales en posesión de las dependencias y entidades, así como establecer los estándares mínimos que deben contener los documentos de seguridad de los Sujetos Obligados; formular observaciones y recomendaciones a los Sujetos Obligados para el cumplimiento o incumplimiento de la Ley de la materia, y llevar a cabo visitas de verificación en materia de seguridad de los sistemas de datos personales en posesión de los Sujetos Obligados, entre otras. Todo lo anterior, entre otras cosas, con el fin de garantizar la seguridad de los sistemas de datos personales.

Que, por medio de la protección de los datos personales, se garantiza a las personas físicas el derecho que tienen para decidir respecto del uso y destino de esa información, con el objeto de que sea utilizada para los fines legales para los que fue entregada a los Sujetos Obligados; se maneje de forma adecuada y segura, y se impida su transmisión ilícita, con la finalidad de salvaguardar la privacidad e intimidad de dichas personas.

Que un aspecto fundamental de la protección de los datos personales es la seguridad de los datos personales.

Que dicha seguridad es una garantía de la integridad, disponibilidad y confidencialidad de la información.

Que, por ello, los Sujetos Obligados deben adoptar, mantener y documentar las medidas de seguridad administrativa, física y técnica necesarias para garantizar la integridad, confidencialidad y disponibilidad de los datos personales, mediante acciones que eviten su daño, alteración, pérdida y destrucción; así como su uso, transmisión y acceso no autorizado, de conformidad con lo previsto en la Ley y demás disposiciones aplicables.

Que la seguridad es uno de los deberes del Sujeto Obligado, la cual se traduce en la obligación de adoptar medidas de seguridad y hacerlas cumplir por quienes traten datos personales bajo su supervisión, ya sean sus empleados o un encargado del tratamiento que acceda a los datos personales para prestarle algún servicio, con el objeto de proteger los datos de carácter personal que someta a tratamiento, mediante la implementación de las medidas técnicas, físicas y organizativas que resulten idóneas para garantizar su integridad, confidencialidad y disponibilidad.

Que, en virtud de este deber, todo Sujeto Obligado que lleve a cabo tratamiento de datos personales deberá establecer y mantener las medidas de seguridad administrativa, física y técnica necesarias para proteger los datos personales contra daño, pérdida, alteración y destrucción; así como su uso, transmisión, acceso o tratamiento no autorizado.

Que, en consecuencia, las medidas de seguridad constituyen un deber y, por lo tanto, se convierten en una obligación del responsable y, en su caso, del encargado del tratamiento del Sujeto Obligado. Al mismo tiempo, representan un derecho en favor de los particulares o titulares de los datos personales.

Que, por ello, las funciones y obligaciones de todos los que intervengan en el tratamiento de datos personales deberán estar claramente definidas en el documento de seguridad al que se refiere la Ley de la materia.

Que la seguridad es un aspecto clave, puesto que tiene por finalidad proteger los datos personales que son objeto de tratamiento y evitar un uso indebido que pudiera causar un daño irreparable a su titular.

Que la seguridad en el tratamiento de datos de carácter personal es vital para garantizar de forma efectiva la privacidad de las personas, mediante el establecimiento de controles o medidas que impidan el acceso indebido a la información.

Que, al propio tiempo, la adecuada garantía de la protección de los datos personales exige que se mantenga la integridad y exactitud de la información personal, de modo que, con estas medidas, se permita evitar la pérdida total o parcial de los datos o su alteración.

Que la Ley no regula las medidas de seguridad que tienen que establecer y mantener los responsables de los sistemas de datos personales, ya que se limita a indicar que "*serán adoptadas en relación con el menor o mayor grado de protección que ameriten los datos personales, y deberán constar por escrito y ser comunicadas al Instituto para su registro*".

En efecto, no en todos los tratamientos de datos personales deben observarse las mismas medidas de seguridad, sino que esto dependerá de la naturaleza de los datos almacenados y de los riesgos a los que estén expuestos, ya provengan de la acción humana, ya del medio físico o natural. Por lo que la atribución de un nivel de seguridad básico, medio o alto se establecerá atendiendo a la naturaleza de la información tratada, en relación con la mayor o menor necesidad de garantizar la integridad o confidencialidad de los datos personales.

Que, en la implementación de las medidas de seguridad, los Sujetos Obligados deberán tomar en consideración, además de lo previsto en la Ley de la materia, los lineamientos y recomendaciones que, en su caso, emita para este fin el Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de México y Municipios, con el objeto de garantizar la confidencialidad, integridad y disponibilidad de los datos personales durante su tratamiento.

Que, por tales razones, resulta necesario y oportuno emitir los presentes Lineamientos, cuyo alcance es ser un instrumento de disposiciones específicas para lograr la mayor protección de los datos personales, para que los Sujetos Obligados puedan lograr un estándar de seguridad al respecto, sin perjuicio de que éstos establezcan medidas adicionales que coadyuven a la mejor protección de los datos personales.

Los presentes Lineamientos tienen por objeto precisar la serie de pasos por seguir para la seguridad de los datos personales en posesión de los Sujetos Obligados de la Ley de Protección de Datos Personales del Estado de México.

Se trata de disposiciones que buscan dar certeza sobre las tareas u obligaciones que los Sujetos Obligados deben observar en materia de medidas de seguridad aplicables a los sistemas de datos personales en su poder, tanto físicos como automatizados. A su vez, estos Lineamientos son un instrumento de verificación para los Sujetos Obligados, ya que permiten facilitar la evaluación, implementación y supervisión de dichas medidas.

De esta forma, los responsables de uno o más sistemas de datos personales podrán determinar con claridad aquellos apartados o disposiciones que resulten aplicables por el nivel de protección de los datos personales y el tipo de sistema.

Es decir, quienes realicen el tratamiento de datos personales en soportes físicos estarán obligados sólo a sujetarse al apartado o disposiciones que regulan o hacen referencia a ese tipo de soportes y, dentro de ese apartado, únicamente a las medidas respectivas al nivel de protección que corresponda; por consiguiente, podrán omitir la revisión de otros apartados que no resulten aplicables a la naturaleza de los datos personales tratados.

Por lo expuesto, el Pleno del Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de México y Municipios ha tenido a bien expedir los siguientes:

LINEAMIENTOS SOBRE MEDIDAS DE SEGURIDAD APLICABLES A LOS SISTEMAS DE DATOS PERSONALES QUE SE ENCUENTRAN EN POSESIÓN DE LOS SUJETOS OBLIGADOS DE LA LEY DE PROTECCIÓN DE DATOS PERSONALES DEL ESTADO DE MÉXICO

TÍTULO PRIMERO
De los sistemas de datos personales

Capítulo Único
De los sistemas de datos personales

De las categorías de datos personales

Artículo 1. Los datos personales contenidos en los sistemas de datos personales se clasificarán, de manera enunciativa y no limitativa, en las siguientes categorías:

I. Datos de identificación: Nombre; domicilio; teléfono particular y/o celular; correo electrónico personal; estado civil; firma; firma electrónica; cartilla militar; lugar y fecha de nacimiento; nacionalidad; edad; fotografía; clave del Registro Federal de Contribuyentes (RFC); Clave Única de Registro de Población (CURP); nombres de familiares, dependientes y beneficiarios; costumbres; idioma o lengua, y voz, entre otros;

II. Datos laborales: Documentos de reclutamiento y selección, de nombramiento, de incidencia y de capacitación; puesto; domicilio de trabajo; correo electrónico institucional; teléfono institucional; actividades extracurriculares; referencias laborales; referencias personales; solicitud de empleo, y hoja de servicio, entre otros;

III. Datos patrimoniales: Bienes muebles e inmuebles; historial crediticio; información fiscal; ingresos y egresos; cuentas bancarias; seguros, afores; fianzas; servicios contratados, y referencias personales, entre otros;

IV. 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, fiscal, administrativa o de cualquier otra rama del Derecho;

V. Datos académicos: Trayectoria educativa; calificaciones; títulos; cédula profesional; certificados, y reconocimientos, entre otros;

VI. Datos de tránsito y movimientos migratorios: Información relativa al tránsito de las personas dentro y fuera del país e información migratoria de las personas, entre otros;

VII. Datos de salud: Estado de salud físico y/o mental; historial o expediente clínico de toda atención médica; referencias o descripción de síntomas, alergias o enfermedades; información relacionada con cuestiones de carácter psicológico y/o psiquiátrico; vacunas; intervenciones quirúrgicas; incapacidades médicas; discapacidades; uso de aparatos oftalmológicos, ortopédicos, auditivos o prótesis, y consumo de sustancias tóxicas y estupefacientes, entre otros;

VIII. Datos ideológicos: Creencias religiosas; ideología; afiliación política y/o sindical, y pertenencia a organizaciones de la sociedad civil y/o asociaciones religiosas, entre otros;

IX. Datos de vida sexual: Preferencia sexual y hábitos sexuales, entre otros;

X. Datos de origen: Información relativa al origen étnico y racial;

XI. Datos biométricos: Información relativa a rasgos característicos y distintivos de partes físicas o biológicas de la persona que la diferencian de las demás y/o que pueden atribuirse a una persona en particular, pues la identifican. Estos datos pueden clasificarse como dinámicos o estáticos:

a) Los datos biométricos dinámicos conciernen a aspectos del comportamiento de la persona; es decir, a ciertas actuaciones que realiza en su ambiente social que la distinguen de los demás. Dentro de éstos, se enmarcan la firma manuscrita; la pulsación sobre las teclas; el análisis de la forma de caminar, y el análisis gestual, entre otros, o

b) Los datos biométricos estáticos corresponden a la anatomía del ser humano; es decir, a los aspectos fisiológicos que son distintivos de cada persona y que se encuentran en ella de forma permanente, sin posibilidad de ser modificados

por la propia voluntad de la persona. Dentro de éstos, se incluyen las huellas digitales; la geometría de la mano; el análisis del iris o de la retina; el reconocimiento facial o del diafragma, y el análisis del ADN, entre otros, y

XII. Datos electrónicos: Direcciones electrónicas, como correo electrónico no oficial; dirección IP (protocolo de internet); dirección MAC (Media Access Control o Control de Acceso al Medio); nombres de usuario; contraseñas; firma electrónica o cualquier otra información empleada por la persona para su identificación en internet u otra red de comunicaciones electrónicas.

El resto de la información que pueda considerarse personal se incluirá en la categoría que le sea más afín a su naturaleza.

Del acuerdo del Sujeto Obligado para crear, modificar o suprimir sistemas de datos personales

Artículo 2. La creación, modificación o supresión de sistemas de datos personales por parte de cada Sujeto Obligado sólo podrá efectuarse mediante acuerdo de su titular o del Comité de Información, debidamente fundado y motivado. Dicho acuerdo será notificado al Instituto dentro del término de 10 días hábiles posteriores a la realización de dicho acto.

Del registro de los sistemas de datos personales
Artículo 3. Una vez que emitan el acuerdo para la creación, modificación o supresión de sistemas de datos personales, los Sujetos Obligados deberán hacer el registro respectivo ante el Instituto, en términos del artículo 52 de la Ley.

Del contenido del acuerdo de creación de un sistema de datos personales
Artículo 4. El acuerdo de creación de sistemas de datos personales deberá contener:

I. La identificación del sistema de datos personales, especificando su denominación y normativa aplicable; así como la descripción de su finalidad y usos previstos;

II. El origen de los datos contenidos en el sistema de datos personales, estableciendo el universo de personas cuya información se pretende obtener o que resulten obligadas a suministrarla; su procedencia (propio interesado, representante, ente público, etcétera) y su procedimiento de obtención (formulario, internet, transmisión electrónica, etcétera);

III. Las cesiones de datos previstas, señalando, en su caso, los destinatarios o categorías de los destinatarios;

IV. La identificación de la Unidad Administrativa a la cual corresponderá el sistema de datos, así como del cargo del responsable;

V. Domicilio oficial y dirección electrónica de la Unidad de Información ante la cual se presentarán las solicitudes para ejercer los derechos de acceso, rectificación, cancelación y oposición, así como la revocación del consentimiento, respecto de los datos contenidos en el sistema de datos personales;

VI. La indicación del nivel de seguridad que sea aplicable al sistema de datos personales (básico, medio o alto), y

VIII. El tiempo de conservación de los datos personales contenidos en el sistema.

Del contenido del acuerdo de modificación
Artículo 5. El acuerdo mediante el cual se determine la modificación de un sistema de datos personales deberá señalar los cambios producidos en cualquiera de las fracciones a las que se refiere el numeral anterior de estos Lineamientos.

Todo acuerdo de modificación que afecte la integración y tratamiento de un sistema de datos personales deberá ser notificado al Instituto, dentro del término de 10 días hábiles siguientes a la realización de dicho acto.

Del contenido del acuerdo de supresión de sistemas de datos personales
Artículo 6. En caso de que el Sujeto Obligado determine la supresión de un sistema de datos personales, el acuerdo correspondiente deberá ser notificado al Instituto dentro del término de 10 días hábiles siguientes, a efecto de que se proceda a la cancelación de la inscripción en el registro respectivo.

En los acuerdos que se emitan para la supresión de sistemas de datos personales, habrá de establecerse el destino que vaya a darse a los datos contenidos en ellos o, en su caso, las previsiones que se adopten para su destrucción.

La supresión de los sistemas de datos personales no procederá cuando exista una previsión expresa en una Ley que exija su conservación.

Título Segundo
De las medidas de seguridad en el tratamiento de datos personales

Capítulo Primero
De los niveles de las medidas de seguridad

De los niveles de seguridad
Artículo 7. En términos del artículo 59, inciso B, de la Ley, las medidas de seguridad se clasificarán en tres niveles: básico, medio y alto.

Dichas medidas serán acumulativas; es decir, el nivel medio comprenderá las medidas del nivel básico, mientras que el nivel alto incluirá tanto las medidas del nivel básico como del nivel medio.

De los niveles de seguridad por categoría de datos

Artículo 8. Las medidas de seguridad aplicables a los sistemas de datos personales responderán a los niveles señalados en la Ley para cada categoría de datos personales. Dichas medidas deberán tomar en consideración las recomendaciones que, en su caso, emita el Instituto para este fin, con el objeto de garantizar la confidencialidad, integridad y disponibilidad de los datos personales durante su tratamiento.

En todo caso, deberán tomarse en cuenta los criterios internacionales establecidos en la materia, sobre medidas de seguridad para el resguardo eficaz de los datos personales.

Al final de cada medida sugerida, se establecen los niveles de seguridad que habrán de observarse, según la naturaleza de la información contenida en los sistemas de datos personales.

Los niveles de seguridad deberán responder a la mayor o menor necesidad de garantizar la integridad de los datos personales.

Los Sujetos Obligados aplicarán el nivel básico, medio o alto de acuerdo con las categorías de datos personales indicadas a continuación:

I. Nivel básico: Estas medidas de seguridad serán aplicables a todos los sistemas de datos personales.

En los sistemas de datos personales que contengan alguna de las categorías de datos que se enlistan a continuación, resultarán aplicables, al menos, las medidas de seguridad de nivel básico:

a) Datos de identificación, y
b) Datos laborales;

II. Nivel medio: En los sistemas de datos personales que contengan alguna de las categorías de datos que aparecen a continuación, resultarán aplicables tanto las medidas de seguridad de nivel básico como las de nivel medio:

a) Datos patrimoniales,
b) Datos sobre procedimientos administrativos seguidos en forma de juicio y/o jurisdiccionales,
c) Datos académicos, y
d) Datos de tránsito y movimientos migratorios, y

III. Nivel alto: En los sistemas de datos personales que contengan alguna de las categorías de datos que aparecen a continuación, resultarán aplicables tanto las medidas de seguridad de nivel básico y medio como las de nivel alto:

a) Datos de salud;
b) Datos ideológicos;
c) Datos de origen;
d) Datos biométricos dinámicos y/o estáticos, y
e) Datos de vida sexual.

De las abreviaturas

Artículo 9. Para efectos de la aplicación de las disposiciones de este título, se deberá estar a las siguientes abreviaturas:

I. La referencia a *medidas de seguridad* se identificará con la abreviatura MS;

II. La referencia a *sistema de datos personales* se identificará con la abreviatura SDP, y

III. La referencia a *sistemas de datos personales* se identificará con la abreviatura SDPS.

De las definiciones

Artículo 10. Para efectos de la aplicación de las disposiciones de este título, además de las definiciones contenidas en el artículo 4 de la Ley, se entenderá por:

I. Área de consulta de datos personales: Espacio destinado para que el personal autorizado examine los datos personales que está autorizado a consultar, sin posibilidad de modificar su contenido;

II. Área de recepción de datos personales: Espacio donde se reciben datos personales en cualquier tipo de soporte (físico, electrónico o ambos), en tanto se siguen las demás fases de su tratamiento, para integrarlos a uno o más SDPS;

III. Área de resguardo de datos personales: Espacio para almacenar datos personales que han recibido el tratamiento correspondiente, para que formen parte integral de uno o más SDPS, sin importar el tipo de soporte (físico, electrónico o ambos) utilizado para su almacenamiento;

IV. Divulgación de incidentes: Acciones que adoptan el titular del Sujeto Obligado y el responsable de los SDPS, a efecto de dar a conocer a las autoridades competentes, a los titulares de los datos y, en su caso, al público en general, los actos deliberados (intrusión, robo, etcétera) y los acontecimientos de caso fortuito o de fuerza mayor (desastres naturales, incendios, huelgas, etcétera) que hubieran ocasionado la pérdida total o parcial de los datos personales bajo su custodia;

V. Intrusión: Acción que una o más personas realizan para introducirse, sin derecho, en uno o más SDPS, a fin de alterar, copiar o sustraer los datos personales que forman parte de dichos sistemas;

VI. Malware: Software malicioso o maligno utilizado por personas para causar daños en una o más computadoras o para sustraer archivos de los equipos; es decir, virus, gusanos cibernéticos, caballos de Troya, *spyware*, *bots* y *rootkits*, además de los que se creen posteriormente con el mismo propósito;

VII. Manual de operaciones: Conjunto de documentos que enumera, define y detalla los procesos y procedimientos que los servidores públicos llevan a cabo dentro de un Sujeto Obligado;

VIII. Personal o personal autorizado: Usuarios o encargados (servidores públicos) que han recibido autorización, por parte del responsable de uno o más SDPS, para interactuar con dichos sistemas;

IX. Personal de sistemas: Personal que labora en el área de tecnologías de información, sistemas, telecomunicaciones u otras análogas;

X. Soportes electrónicos: Medios de almacenamiento inteligibles sólo mediante el uso de algún aparato con circuitos electrónicos que procese su contenido para examinar, modificar o almacenar los datos; es decir, cintas magnéticas de audio, video y datos; fichas de microfilm; discos ópticos (CD y DVD); discos magneto-ópticos; discos magnéticos (flexibles y duros), y demás medios de almacenamiento masivo no volátil;

XI. Soportes físicos: Medios de almacenamiento inteligibles a simple vista; es decir, que no requieren de ningún aparato que procese su contenido para examinar, modificar o almacenar los datos; es decir, formularios impresos llenados "a mano" o "a máquina", fotografías y placas radiológicas, entre otros;

XII. Supervisión interna: Proceso sistemático mediante el cual se realiza la recopilación, acumulación y evaluación de evidencia sobre la adopción y práctica de las MS recomendadas en este documento por parte de un Sujeto Obligado. Sus propósitos son precisar e informar el grado de cumplimiento entre la información recabada y los criterios establecidos, y

XIII. Zona de acceso restringido: Todas aquellas áreas a las que únicamente tienen acceso el personal autorizado y el personal de vigilancia; es decir, las áreas de recepción, resguardo y consulta de datos personales.

Capítulo Segundo
De las reglas generales de las medidas de seguridad

De las medidas de seguridad

Artículo 11. Las MS que adopten los Sujetos Obligados para los SDPS en su poder deberán atender los aspectos o previsiones generales previstas en la Ley y por estos Lineamientos, sin perjuicio de las disposiciones o aspectos específicos que se determinen más adelante en estos Lineamientos. Los aspectos generales atenderán a lo siguiente:

I. Nivel básico: Este nivel de seguridad será aplicable a todos los SDPS y comprenderá los siguientes aspectos:

a) **Documento de seguridad:** El Sujeto Obligado elaborará el documento de seguridad que será de observancia obligatoria para todos los servidores públicos que lo conforman, así como para todas las personas que, debido a la prestación de un servicio, tengan acceso a los SDPS y/o al sitio donde éstos se ubican, tomando en cuenta lo dispuesto en la Ley y en estos Lineamientos.

   El documento de seguridad deberá contener los requisitos establecidos en el artículo 63 de la Ley; asimismo, deberá actualizarse anualmente o cuando se produzcan cambios relevantes en el tratamiento que puedan repercutir en el cumplimiento de las MS implantadas;

b) **Funciones u obligaciones del personal que intervenga en el tratamiento de los SDPS:** Estas funciones y obligaciones deberán estar claramente definidas en el documento de seguridad.

   El responsable adoptará las medidas necesarias para que el personal conozca las normas de seguridad que afecten el desarrollo de sus funciones, así como las responsabilidades y consecuencias que puedan derivarse de su incumplimiento;

c) **Registro de incidencias:** Los procedimientos de notificación, gestión y respuesta ante incidencias contarán necesariamente con un registro, en el cual se harán constar el tipo de incidencia, el momento en que se ha producido, la persona que realiza la notificación, la persona a quien se le comunica, los efectos que se deriven de ella y las acciones implementadas;

d) **Identificación y autenticación:** El responsable tendrá a su cargo la elaboración de una relación actualizada de los servidores públicos que tengan acceso autorizado a los SDPS y del establecimiento de procedimientos que permitan la correcta identificación y autenticación para dicho acceso.

El responsable establecerá un mecanismo que permita la identificación, de forma inequívoca y personalizada, de toda persona que intente acceder a los SDPS y la verificación de que está autorizada.

Cuando el mecanismo de autenticación se base en la existencia de contraseñas, se establecerá un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad.

Las contraseñas se cambiarán con la periodicidad que se determine en el documento de seguridad y se conservarán cifradas.

Asimismo, se establecerá un procedimiento de creación y modificación de contraseñas (longitud, formato y contenido);

e) **Control de acceso:** El responsable deberá adoptar las medidas necesarias para que los encargados y usuarios tengan acceso autorizado únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones.

El responsable deberá mantener una relación actualizada de personas autorizadas y los accesos autorizados para cada una de ellas. Asimismo, deberá establecer los procedimientos para el uso de bitácoras respecto de las acciones cotidianas llevadas a cabo en los SDPS.

Solamente el responsable podrá conceder, alterar o anular la autorización para el acceso a los SDPS;

f) **Gestión de soportes:** Al almacenar los soportes físicos y electrónicos que contengan datos de carácter personal, se deberá cuidar que estén etiquetados, para permitir identificar el tipo de información que contienen, y ser inventariados. Asimismo, sólo podrán ser accesibles para el personal autorizado para ello en el documento de seguridad.

La salida de soportes y documentos que contengan datos de carácter personal de las instalaciones u oficinas bajo el control del responsable deberá ser autorizada por éste o encontrarse debidamente autorizada en el documento de seguridad.

En el traslado de soportes físicos y electrónicos, se adoptarán las medidas necesarias para evitar la sustracción, pérdida o acceso indebido a la información durante su transporte.

Siempre que vaya a desecharse cualquier soporte que contenga datos de carácter personal, deberá procederse a su destrucción o borrado, mediante la adopción de las medidas dirigidas a evitar el acceso a la información contenida en tal soporte o su recuperación posterior, y

g) **Copias de respaldo y recuperación:** Deberán elaborarse procedimientos para la realización de copias de respaldo y su periodicidad. En caso de que los datos personales se encuentren en soporte físico, se procurará que el respaldo se efectúe mediante la digitalización de los documentos.

Asimismo, para los soportes electrónicos, se establecerán procedimientos para la recuperación de los datos que garanticen, en todo momento, su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida involuntaria o destrucción accidental.

El responsable se encargará de verificar, al menos cada seis meses, la correcta definición, funcionamiento y aplicación de los procedimientos de realización de copias de respaldo y de recuperación de los datos.

II. **Nivel medio:** El nivel de seguridad medio, además de las MS previstas para el nivel básico, deberá comprender:

a) **Responsable de seguridad:** El responsable designará uno o varios responsables de seguridad, para coordinar y controlar las medidas definidas en el documento de seguridad. Esta designación podrá ser única para todos los SDPS en posesión del Sujeto Obligado o diferenciada, según los métodos de organización y tratamiento de datos personales. En todo caso, dicha circunstancia deberá especificarse en el documento de seguridad.

En ningún caso, esta designación supondrá una delegación de las facultades y atribuciones de que corresponden al responsable de los SDPS, de acuerdo con la Ley y estos Lineamientos;

b) **Auditoría:** Las MS implementadas para la protección de los SDPS se someterán a una auditoría interna o externa, para verificar el cumplimiento de la Ley, de estos Lineamientos y demás procedimientos vigentes en materia de seguridad de datos, al menos cada dos años.

El informe de resultados de la auditoría deberá dictaminar sobre la adecuación de las MS previstas en estos Lineamientos, así como las recomendaciones que, en su caso, haya emitido el Instituto. Además, deberá identificar sus deficiencias y proponer las medidas preventivas, correctivas o complementarias necesarias.

El informe de resultados de la auditoría deberá ser comunicado por el responsable al Instituto, dentro de los 20 días hábiles siguientes a su emisión. Asimismo, se deberá informar al Instituto de la adopción de las medidas correctivas derivadas de la auditoría en el plazo referido, a partir de que éstas hayan sido atendidas;

c) **Control de acceso físico:** El acceso a las instalaciones donde se encuentren los SDPS, ya sea en soporte físico o electrónico, deberá permitirse exclusivamente a quienes estén expresamente autorizados en el documento de seguridad, y

d) **Pruebas con datos reales:** Las pruebas que se lleven a cabo para verificar la correcta aplicación y funcionamiento de los procedimientos para la obtención de copias de respaldo y de recuperación de los datos, anteriores a la implantación o modificación de los sistemas informáticos que traten SDPS, no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente al tipo de datos tratados. Si se realizan pruebas con datos reales, se elaborará una copia de respaldo con anterioridad.

III. Nivel alto: El nivel de seguridad alto, además de las MS previstas para el nivel básico y el nivel medio, deberá comprender:

a) **Distribución de soportes:** La distribución de los soportes que contengan datos de carácter personal se realizará cifrando dichos datos, o bien, utilizando cualquier otro mecanismo que garantice la integridad y confidencialidad de la información durante su traslado o transmisión;

b) **Registro de acceso:** El acceso a los SDPS se limitará exclusivamente al personal autorizado, estableciendo los mecanismos que permitan identificar los accesos realizados, en caso de que los sistemas puedan ser utilizados por múltiples autorizados.

Los mecanismos para el registro de acceso estarán bajo el control directo del responsable de seguridad correspondiente, sin que se permita su desactivación o manipulación.

De cada acceso se guardarán, al menos, la identificación del usuario, la fecha y hora en que se realizó, el sistema accedido, el tipo de acceso y si éste fue autorizado o denegado.

El periodo de conservación de los datos consignados en el registro de acceso será de, al menos, dos años, y

c) **Telecomunicaciones:** La transmisión de datos de carácter personal a través de redes públicas o de redes inalámbricas de comunicaciones electrónicas se realizará cifrando dichos datos, o bien, utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulable por terceros.

De la notificación del nivel de seguridad
Artículo 12. Los responsables deberán comunicar al Instituto el nivel de seguridad aplicable a los SDPS para su registro.

De las prestaciones de servicios sin acceso a datos personales
Artículo 13. El responsable adoptará las medidas necesarias para limitar el acceso de cualquier persona a los SDPS, para la realización de trabajos que no impliquen el tratamiento de datos personales.

Cuando se trate de personal ajeno, el contrato de prestación de servicios deberá contener una cláusula expresa sobre la prohibición de acceder a los datos personales y la obligación de secreto respecto de los datos que hubiera podido conocer con motivo de la prestación del servicio.

Del tratamiento de las bases de datos fuera de las oficinas del responsable
Artículo 14. Cuando los datos personales se almacenen en dispositivos portátiles o se traten fuera de las oficinas del responsable, será preciso que exista una autorización previa por parte de éste y, en todo caso, deberá garantizarse el nivel de seguridad correspondiente al tipo de sistema de que se trate.

La autorización a la que se refiere el párrafo anterior tendrá que constar en el documento de seguridad y podrá establecerse para un usuario o para un perfil de usuarios, además de determinar un periodo de validez para tal autorización.

De las medidas de seguridad aplicables a los archivos físicos
Artículo 15. Además de las medidas adoptadas por cada nivel de seguridad, los archivos físicos o no automatizados deberán soportar y conservar los documentos que generen en términos de la Ley de Documentos Administrativos e Históricos del Estado de México y de los criterios que al respecto emita el Instituto.

De los dispositivos de almacenamiento
Artículo 16. Los dispositivos de almacenamiento de los documentos que contengan datos de carácter personal deberán disponer de mecanismos que obstaculicen su apertura.

Cuando las características físicas de aquéllos no permitan adoptar esta medida, el responsable adoptará las medidas que impidan el acceso de personas no autorizadas.

De la custodia de los soportes

Artículo 17. Mientras la documentación con datos de carácter personal no se encuentre archivada en los dispositivos de almacenamiento establecidos en el artículo anterior, por estar en proceso de revisión o tramitación, ya sea previo o posterior a su archivo, la persona que se encuentre a cargo de la información deberá custodiarla e impedir, en todo momento, que pueda ser accedida por personas no autorizadas.

Del almacenamiento de la información

Artículo 18. Los armarios, archiveros u otros elementos en los que se almacenen los documentos con datos de carácter personal deberán encontrarse en áreas en las que el acceso esté protegido con puertas de acceso dotadas de sistemas de apertura mediante llave u otro dispositivo equivalente. Dichas áreas deberán permanecer cerradas cuando no sea preciso el acceso a los documentos.

Si no es posible disponer de un área resguardada para los archivos que contengan datos personales, el responsable adoptará medidas alternativas que, debidamente motivadas, se incluirán en el documento de seguridad.

De la copia o reproducción

Artículo 19. La generación de copias o la reproducción de los documentos únicamente podrá ser realizada bajo el control del personal autorizado en el documento de seguridad.

Una vez cumplido el objeto por el cual se generó la copia o reproducción, ésta deberá destruirse, de modo que se evite el acceso a la información contenida en ella o su recuperación posterior.

Del traslado de documentación

Artículo 20. Siempre que se proceda al traslado físico de la documentación contenida en un archivo, deberán adoptarse medidas dirigidas a impedir el acceso o manipulación de la información objeto de traslado.

Capítulo Tercero
De las medidas de seguridad para datos personales en soportes físicos

Sección Primera
Del área de recepción de datos personales

Del área de recepción

Artículo 21. En el espacio destinado a la recepción de datos personales en soporte físico, se deberá observar lo siguiente, según corresponda:

I. Que exista la infraestructura apropiada, así como los procesos y procedimientos necesarios y suficientes, que hagan posible mantener, en forma organizada y segura, los datos personales recibidos en el área de recepción, en tanto se siguen las demás fases de su tratamiento (nivel básico);

II. Que el personal autorizado que labora en el área de recepción ostente una identificación con fotografía (credencial o gafete) emitida por el Sujeto Obligado (nivel básico);

III. Que cualquier persona pueda 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);

IV. Que el encargado de los SDPS actualice los nombres completos y fotografías que se exhiben en el área de recepción, conforme se presenten cambios de personal (nivel medio);

V. Que no se permita el libre acceso y uso de aquellos aparatos referidos en la sección sexta del capítulo sexto de este título, relativa a "equipo no autorizado" dentro del área de recepción (nivel medio), y

VI. Que exista señalización visible sobre las restricciones de acceso, prohibiciones que aplican y procedimiento para dar aviso al personal de vigilancia, en caso de sospecharse la presencia de personas no autorizadas en el área de recepción (nivel básico).

Sección Segunda
Del área de resguardo de datos personales

Del área de resguardo

Artículo 22. En el espacio destinado para almacenar o resguardar datos personales que han recibido el tratamiento correspondiente, para que formen parte integral de uno o más SDPS en soporte físico, se deberá observar lo siguiente, según corresponda:

I. Que exista la infraestructura apropiada, así como los procesos y procedimientos necesarios y suficientes, que hagan posible mantener, en forma organizada y segura, los soportes físicos que contengan datos personales dentro del área de resguardo (nivel básico);

II. Que, de existir ventanas o muros divisorios transparentes en el área de resguardo, la visión quede obstruida con una película translúcida, como papel albanene (nivel medio);

III. Que, al interior del área de resguardo, existan las condiciones ambientales idóneas para preservar en buen estado los soportes físicos que contengan datos personales, durante el tiempo de conservación (nivel básico);

IV. Que la puerta de acceso del área de resguardo cuente con cerradura, dispositivo electrónico o cualquier otra tecnología que impida su libre apertura. Este mecanismo deberá quedar cerrado en horas no hábiles o cuando el personal autorizado que ahí labora abandone el área (nivel básico);

V. Que el mobiliario utilizado dentro del área de resguardo proteja los soportes físicos que contengan datos personales de condiciones adversas de humedad, temperatura, luz solar, polvo, consumo de alimentos y presencia de plagas, entre otros factores de riesgo (nivel básico);

VI. Que el mobiliario utilizado para almacenar los soportes físicos que contengan datos personales cuente con cerraduras, dispositivos electrónicos o cualquier otra tecnología que impida la libre apertura de sus puertas, cajones o compartimientos. Tales mecanismos deberán quedar cerrados en horas no hábiles (nivel medio);

VII. Que el personal autorizado que labora en el área de resguardo ostente una identificación con fotografía (credencial o gafete) emitida por el Sujeto Obligado (nivel básico);

VIII. Que cualquier persona pueda 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 (nivel medio);

IX. Que el encargado de los SDPS actualice los nombres completos y fotografías que se exhiben en el área de resguardo, conforme se presenten cambios de personal (nivel medio);

X. Que no esté permitido el libre acceso y uso de aquellos aparatos referidos en la sección sexta del capítulo sexto de este título, relativa a "equipo no autorizado" dentro del área de resguardo (nivel medio), y

XI. Que exista señalización visible sobre las restricciones de acceso, prohibiciones que aplican y procedimiento para dar aviso al personal de vigilancia, en caso de sospecharse la presencia de personas no autorizadas en el área de resguardo (nivel básico).

Sección Tercera
Del área de consulta de datos personales

Del área de consulta

Artículo 23. En el espacio destinado para que el personal autorizado examine aquellos datos personales que esté autorizado a consultar, sin posibilidad de modificar su contenido, se deberá observar lo siguiente, según corresponda:

I. Que exista la infraestructura apropiada, así como los procesos y procedimientos necesarios y suficientes, que hagan posible supervisar y vigilar los soportes físicos que contengan datos personales y a los que accedan los usuarios dentro del área de consulta (nivel básico);

II. Que, de existir ventanas o muros divisorios transparentes en el área de consulta, la visión quede obstruida con una película translúcida, como papel albanene (nivel medio);

III. Que la puerta de acceso del área de consulta cuente con cerradura, dispositivo electrónico o cualquier otra tecnología que impida su libre apertura. Este mecanismo deberá quedar cerrado en horas no hábiles o cuando el personal autorizado que ahí labora abandone el área (nivel medio);

IV. Que el personal autorizado que labora en el área de consulta ostente una identificación con fotografía (credencial o gafete) emitida por el Sujeto Obligado (nivel básico);

V. Que cualquier persona pueda 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 (nivel medio);

VI. Que el encargado de los SDPS actualice los nombres completos y fotografías que se exhiben en el área de consulta, conforme se presenten cambios de personal (nivel medio);

VII. Que no esté permitido el libre acceso y uso de aquellos aparatos referidos en la sección sexta del capítulo sexto de este título, relativa a "equipo no autorizado" dentro del área de consulta (nivel medio), y

VIII. Que existe señalización visible sobre los horarios de atención, restricciones de acceso, prohibiciones que aplican y procedimiento para dar aviso al personal de vigilancia, en caso de sospecharse la presencia de personas no autorizadas en el área de consulta (nivel básico).

Sección Cuarta
Del acceso y consulta de datos personales

Del acceso y consulta
Artículo 24. A las áreas de recepción, de resguardo o consulta de datos personales, sólo tendrán acceso el personal autorizado y el personal de vigilancia. En todo caso, para el acceso, deberá observarse lo siguiente, según corresponda:

I. Que, en las instalaciones del Sujeto Obligado, existan puntos de revisión en los cuales el personal de vigilancia controle el acceso y verifique la identidad de quienes tienen el propósito de ingresar a una zona de acceso restringido (nivel básico);

II. Que el personal que tenga la intención de ingresar a una zona de acceso restringido se registre o entregue una identificación oficial con fotografía (credencia de elector, pasaporte o documento semejante) al personal de vigilancia que atiende dicho punto de revisión (nivel medio);

III. Que el encargado de los SDPS sea el único que autorice la entrada al área de recepción y de resguardo al personal debidamente registrado, anotando tal circunstancia o hecho en términos de lo previsto en la sección quinta del capítulo tercero de este título, relativa a "registro de actividades" (nivel básico), y

IV. Que el Sujeto Obligado adopte las MS necesarias para el ingreso a las zonas de acceso restringido.

De la consulta
Artículo 25. Para la consulta de datos personales, deberá observarse lo siguiente, según corresponda:

I. Que, al autorizar la salida de soportes electrónicos o físicos que contengan datos personales, el encargado de los SDPS registre dicha circunstancia o hecho en términos de lo previsto por la sección quinta del capítulo tercero de este título, relativa a "registro de actividades" (nivel básico), y

II. Que el usuario consulte los soportes físicos que contengan datos personales dentro del área de consulta (nivel alto).

De las personas autorizadas y no autorizadas
Artículo 26. El ingreso a las zonas de acceso restringido en las que existan soportes físicos que contengan datos personales se realizará sólo con la autorización de los encargados de los SDPS (nivel básico).

Cada acceso y consulta realizada por personas no autorizadas se considerará como un incidente de intrusión y deberá denunciarse ante las instancias competentes para su investigación (nivel medio).

De las medidas para la prevención de intrusiones
Artículo 27. Con el fin de prevenir intrusiones en los SDPS, los Sujetos Obligados deberán tomar las siguientes medidas, según corresponda:

I. El personal autorizado que labora en las zonas de acceso restringido deberá verificar, en el desempeño de sus funciones, que en dichas áreas no haya personas no autorizadas (nivel básico);

II. El personal de vigilancia deberá realizar funciones de manera permanente en las zonas de acceso restringido (nivel medio);

III. Las zonas de acceso restringido deberán contar con un sistema de videovigilancia remota, que permita supervisar la puerta de acceso y el interior de las referidas áreas. Dicho sistema deberá contar con cámaras para visión nocturna, sistema de grabación que opere las 24 horas y los 7 días de la semana (24x7) y un archivo que acumule las grabaciones de los dos meses anteriores (nivel alto), y

IV. En caso de que ocurra un incidente de intrusión, el personal de vigilancia deberá acudir de inmediato a la zona de acceso restringido presuntamente violada, con el fin de corroborar el hecho. Si éste se comprueba, la grabación realizada por el sistema de videovigilancia se transferirá a un soporte físico, para que pueda utilizarse como prueba por las autoridades que investiguen el caso (nivel alto).

Sección Quinta
Del registro de actividades

De la operación cotidiana
Artículo 28. El responsable de los SDPS mantendrá un estricto control y registro de:

I. Las autorizaciones emitidas para facultar a un servidor público como usuario para interactuar con uno o más SDPS, ya sea que dicho servidor público lo haga acudiendo al área de consulta o desde otro lugar distinto, fuera de dicha área (nivel básico);

II. La asignación, actualización y remplazo de llaves, tarjetas, contraseñas de acceso y demás elementos que entregue a los usuarios, para que éstos puedan activar los mecanismos de apertura de puertas y mobiliario en las zonas de acceso restringido (nivel básico);

III. Las autorizaciones emitidas a los usuarios y demás personal debidamente registrado que soliciten acceso a las áreas de recepción o resguardo. Para ello, el encargado deberá anotar:

a) Quién solicita el acceso,
b) Cuándo solicita el acceso,
c) Cuándo se lleva a cabo el acceso, y
d) La razón que motiva el acceso (nivel básico);

IV. Las autorizaciones emitidas a los usuarios que soliciten permiso para extraer soportes físicos que contengan datos personales del área de consulta. Para ello, el encargado deberá anotar:

a) Quién hace la solicitud,
b) Qué documentos se lleva,
c) Cuándo se los lleva,
d) Cuándo promete devolverlos (si aplica),
e) Cuándo efectivamente los devuelve (si aplica), y
f) Por qué necesita llevárselos (nivel medio);

V. Las autorizaciones emitidas a los usuarios que soliciten permiso para introducir a las zonas de acceso restringido aparatos como los mencionados en la sección sexta del capítulo sexto de este título, relativa a "equipo no autorizado". Para ello, el encargado deberá anotar:

a) Quién hace la solicitud,
b) Qué equipo introduce,
c) Cuándo y por cuánto tiempo,
d) Por qué necesita introducirlo (nivel medio), y

VI. El sistema de videovigilancia remota deberá registrar las actividades diarias, así como los incidentes en las zonas de acceso restringido (nivel alto).

Sección Sexta
De la divulgación de incidentes

Del procedimiento en caso de incidentes

Artículo 29. En caso de que se presente un incidente, se seguirá el procedimiento que el Sujeto Obligado tenga definido (nivel básico).

En todo caso, dicho procedimiento deberá incluir las siguientes actividades, sin necesidad de que se realicen en el orden en que aparecen:

I. El responsable del personal de vigilancia deberá emitir un informe al responsable de los SDPS, en un plazo no mayor a 3 días naturales de haber ocurrido el incidente (nivel básico);

II. En caso de robo o extravío de datos personales en soportes físicos, el titular del Sujeto Obligado y/o el responsable de los SDPS, al tener conocimiento del incidente, deberá dar vista al órgano interno de control, al área jurídica y/o al servidor público que cuente con las facultades para presentar denuncias o querellas de cada Sujeto Obligado, en términos de sus reglamentos interiores o estatutos orgánicos, según corresponda, para que cada uno, en el ámbito de sus atribuciones, determine lo conducente (nivel básico);

III. En un plazo no mayor a 3 días naturales de haber ocurrido el incidente, el responsable de los SDPS deberá dar aviso al público, mediante un desplegado de prensa que difunda dicha circunstancia o hecho por diversos medios, según la gravedad del caso, a escala local, regional, municipal o nacional (nivel medio), y

IV. En caso de robo o extravío de datos personales, se alertará 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 SDPS deberá avisar por escrito a dichos titulares, a más tardar 5 días naturales tras haber ocurrido el incidente, recabando el acuse de recibo de esta notificación. Con anticipación a dicho escrito, si se cuenta con los datos actualizados, se deberá dar aviso por correo electrónico o por teléfono a dichos titulares (nivel básico).

De la supervisión

Artículo 30. El Comité de Información del Sujeto Obligado deberá proponer la realización de, al menos, una supervisión interna para las Unidades Administrativas que mantienen y operan los SDPS (nivel básico).

Sección Séptima
De la baja de datos personales

De la baja de datos personales

Artículo 31. Para proceder a la baja documental de soportes físicos que contengan datos de carácter personal, deberán observarse las disposiciones establecidas al respecto, para la organización y conservación de los archivos en posesión de los Sujetos Obligados y, además:

I. El encargado de los SDPS deberá:

a) Seguir los procedimientos y utilizar los mecanismos para asegurar la valoración y, en su caso, destrucción de soportes físicos que contengan datos personales (nivel medio),
b) Destruir por completo dichos soportes físicos antes de desecharlos (nivel básico), y
c) Llevar una bitácora de las veces que se efectúa la acción de baja de datos personales (nivel básico).

De los métodos de destrucción

II. Los métodos de destrucción de datos personales en soportes físicos estarán definidos en el manual de operaciones del Sujeto Obligado o, si no lo están, deberán ser aprobados por el responsables de los SDPS antes de ejecutarlos (nivel básico).

Del material reciclable con datos personales

III. Si el Sujeto Obligado realiza la separación de materiales para su reciclaje (como papel, cartón, metal o plástico), los materiales reciclables que contengan datos personales deberán ser triturados. La viruta resultante se entregará directamente a una empresa que la reciba para procesarla de inmediato, garantizando por escrito que no será examinada para su eventual reconstrucción (nivel medio).

Capítulo Cuarto
De las medidas de seguridad para datos personales en soportes electrónicos

Sección Primera
Del área de recepción de datos personales

Del área de recepción

Artículo 32. En el espacio destinado a la recepción de soportes electrónicos que contengan datos personales, se deberá observar lo siguiente, según corresponda:

I. Que exista la infraestructura apropiada, así como los procesos y procedimientos necesarios y suficientes, que hagan posible mantener, en forma organizada y segura, los datos personales recibidos en el área de recepción, en tanto siguen las demás fases de su tratamiento (nivel básico);

II. Que el equipo de cómputo instalado en el área de recepción cumpla las disposiciones previstas en el capítulo sexto de este título, relativo a "Medidas de seguridad para equipo de cómputo en zonas de acceso restringido" (nivel básico);

III. Que dicho equipo de cómputo esté 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, tal personal acceda al equipo, a fin de realizar el tratamiento que corresponda a la recepción de datos personales (nivel medio);

IV. Que el personal autorizado que labora en el área de recepción ostente una identificación con fotografía (credencial o gafete) emitida por el Sujeto Obligado (nivel básico);

V. Que cualquier persona pueda 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);

VI. Que el encargado de los SDPS actualice los nombres completos y fotografías que se exhiben en el área de recepción, conforme se presenten cambios de personal (nivel medio);

VII. Que no esté permitido el libre acceso y uso de aquellos aparatos referidos en la sección sexta del capítulo sexto de este título, relativa a "Equipo no autorizado" dentro del área de recepción (nivel medio), y

VIII. Que exista señalización visible sobre las restricciones de acceso, prohibiciones que aplican y procedimiento para dar aviso al personal de vigilancia, en caso de sospecharse la presencia de personas no autorizadas en el área de recepción (nivel básico).

Sección Segunda
Del área de resguardo de datos personales

Del área de resguardo

Artículo 33. En el espacio destinado para almacenar o resguardar datos personales que han recibido el tratamiento correspondiente, para que formen parte integral de uno o más SDPS en soporte electrónico, se deberá observar lo siguiente, según corresponda:

I. Que exista la infraestructura apropiada, así como los procesos y procedimientos necesarios y suficientes, que hagan posible mantener, en forma organizada y segura, los soportes electrónicos que contengan datos personales dentro del área de resguardo (nivel básico);

II. Que, de existir ventanas o muros divisorios transparentes en el área de resguardo, la visión deberá estar obstruida con una película translúcida, como papel albanene (nivel medio);

III. Que, al interior del área de resguardo, existan las condiciones ambientales idóneas para preservar en buen estado los soportes electrónicos que contengan datos personales, durante el tiempo de conservación (nivel básico);

IV. Que la puerta de acceso del área de resguardo cuente con cerradura, dispositivo electrónico o cualquier otra tecnología que impida su libre apertura. Este mecanismo deberá quedar cerrado en horas no hábiles o cuando el personal autorizado que ahí labora abandone el área (nivel básico);

V. Que el equipo de cómputo instalado en el área de resguardo cumpla las disposiciones del capítulo sexto de este título, relativo a "Medidas de seguridad para equipo de cómputo en zonas de acceso restringido" (nivel básico);

VI. Que dicho equipo de cómputo esté 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 acceda al equipo, a fin de realizar el tratamiento que corresponda al resguardo de datos personales (nivel medio);

VII. Que el mobiliario utilizado dentro del área de resguardo proteja los soportes electrónicos que contengan datos personales de condiciones adversas de humedad, temperatura, luz solar, polvo, consumo de alimentos y presencia de plagas, entre otros factores de riesgo (nivel básico);

VIII. Que el mobiliario utilizado para almacenar los soportes electrónicos que contengan datos personales cuente con cerraduras, dispositivos electrónicos o cualquier otra tecnología que impida la libre apertura de sus puertas, cajones o compartimientos. Tales mecanismos deberán quedar cerrados en horas no hábiles (nivel básico);

IX. Que el personal autorizado que labora en el área de resguardo ostente una identificación con fotografía (credencial o gafete) emitida por el Sujeto Obligado (nivel básico);

X. Que cualquier persona pueda 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 (nivel medio);

XI. Que el encargado de los SDPS actualice los nombres completos y fotografías que se exhiben en el área de resguardo, conforme se presenten cambios de personal (nivel medio);

XII. Que no esté permitido el libre acceso y uso de aquellos aparatos referidos en la sección sexta del capítulo sexto de este título, relativa a "equipo no autorizado" dentro del área de resguardo (nivel básico), y

XIII. Que exista señalización visible sobre las restricciones de acceso, prohibiciones que aplican y procedimiento para dar aviso al personal de vigilancia, en caso de sospecharse la presencia de personas no autorizadas en el área de resguardo (nivel básico).

Sección Tercera
Del área de consulta de datos personales

Del área de consulta

Artículo 34. En el espacio destinado para que el personal autorizado examine aquellos datos personales que esté autorizado a consultar, sin posibilidad de modificar su contenido, se deberá observar lo siguiente, según corresponda:

I. Que exista la infraestructura apropiada, así como los procesos y procedimientos necesarios y suficientes, que hagan posible supervisar y vigilar los soportes electrónicos que contengan datos personales y consulten los usuarios de los datos dentro del área de consulta (nivel básico);

II. Que, de existir ventanas o muros divisorios transparentes en el área de consulta, la visión deberá estar obstruida con una película translúcida, como papel albanene (nivel medio);

III. Que la puerta de acceso del área de consulta cuente con cerradura, dispositivo electrónico o cualquier otra tecnología que impida su libre apertura. Este mecanismo deberá quedar cerrado en horas no hábiles o cuando el personal autorizado que ahí labora abandone el área (nivel medio);

IV. Que el equipo de cómputo instalado en el área de consulta cumpla las disposiciones previstas en el capítulo sexto de este título, relativo a "Medidas de seguridad para equipo de cómputo en zonas de acceso restringido" (nivel básico);

V. Que dicho equipo de cómputo esté provisto de la tecnología necesaria y suficiente para verificar la identidad de los usuarios que laboran en el área de consulta. Ello implica que, mediante la verificación de claves de acceso, dicho personal acceda al equipo, a fin de realizar la consulta de datos personales (nivel medio);

VI. Que los usuarios que laboran en el área de consulta ostenten una identificación con fotografía (credencial o gafete) emitida por el Sujeto Obligado (nivel básico);

VII. Que cualquier persona pueda 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 (nivel medio);

VIII. Que el encargado de los SDPS actualice los nombres completos y fotografías que se exhiben en el área de consulta, conforme se presenten cambios de personal (nivel medio);

IX. Que no esté permitido el libre acceso y uso de aquellos aparatos referidos en la sección sexta del capítulo sexto de este título, relativa a "equipo no autorizado" dentro del área de consulta (nivel medio), y

X. Que exista señalización visible sobre horarios de atención, restricciones de acceso, prohibiciones que aplican y procedimiento para dar aviso al personal de vigilancia, en caso de sospecharse la presencia de personas no autorizadas en el área de consulta (nivel básico).

Sección Cuarta
Del acceso y consulta de datos personales

Del acceso

Artículo 35. A las áreas de recepción, de resguardo y de consulta de datos personales, sólo tendrán acceso el personal autorizado y el personal de vigilancia. En todo caso, para el acceso, deberá observarse lo siguiente, según corresponda:

I. Que, en las instalaciones del Sujeto Obligado, existan puntos de revisión en los cuales el personal de vigilancia controle el acceso y verifique la identidad de quienes tengan el propósito de ingresar a una zona de acceso restringido (nivel básico);

II. Que el personal que tenga la intención de ingresar a una zona de acceso restringido se registre y entregue una identificación oficial con fotografía (credencial de elector, pasaporte o documento semejante) al personal de vigilancia que atiende dicho punto de revisión (nivel medio);

III. Que el encargado de los SDPS sea el único que autorice la entrada a las áreas de recepción y resguardo al personal debidamente registrado, anotando dichas circunstancias o hechos, en términos de lo dispuesto en este capítulo, relativo a "registro de actividades" (nivel básico), y

IV. En todo caso, el Sujeto Obligado deberá adoptar las MS necesarias para el ingreso a las zonas de acceso restringido.

De la consulta

Artículo 36. Para la consulta de soportes electrónicos que contengan datos personales, deberá observarse lo siguiente, según corresponda:

I. Que el usuario examine los soportes electrónicos que contengan datos personales dentro del área de consulta (nivel medio), y

II. Que, al autorizar la salida de soportes físicos o electrónicos que contengan datos personales, el encargado de los SDPS anote dichas circunstancias o hechos, en términos de lo dispuesto en este capítulo, relativo a "registro de actividades" (nivel básico).

De las personas autorizadas y no autorizadas

Artículo 37. El ingreso a las zonas de acceso restringido en las que existan soportes electrónicos que contengan datos personales será sólo con autorización del responsable de los SDPS (nivel básico).

Cada acceso y consulta realizada por personas no autorizadas se considerará como un incidente de intrusión, que deberá ser denunciado ante las autoridades competentes para su investigación (nivel básico).

De las medidas para la prevención de intrusiones

Artículo 38. El Sujeto Obligado deberá tomar las siguientes medidas para la prevención de intrusiones en soportes electrónicos para su uso en zonas de acceso restringido:

I. El personal autorizado que labora en las zonas de acceso restringido deberá verificar, en el desempeño de sus funciones, que en dichas áreas no haya personas no autorizadas (nivel básico);

II. El personal de vigilancia deberá realizar funciones de manera permanente en las zonas de acceso restringido (nivel medio);

III. El equipo de cómputo instalado en las zonas de acceso restringido deberá cumplir las disposiciones del capítulo sexto de este título, relativo a "Medidas de seguridad para equipo de cómputo en zonas de acceso restringido" (nivel básico);

IV. Dicho equipo de cómputo deberá estar 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 acceda al equipo para interactuar con el o los SDPS que tiene autorizados (nivel medio);

V. Las zonas de acceso restringido deberán contar con un sistema de videovigilancia remota que permita vigilar la puerta de acceso y el interior de dichas áreas. Dicho sistema deberá contar con cámaras para visión nocturna, sistema de grabación que opere las 24 horas de los 7 días de la semana (24x7) y un archivo que acumule las grabaciones de los dos meses anteriores (nivel alto), y

VI. En caso de que ocurra un incidente de intrusión, el personal de vigilancia deberá acudir de inmediato a la zona de acceso restringido presuntamente violada, para corroborar la circunstancia o el hecho. Si éste se comprueba, la grabación realizada por

el sistema de videovigilancia remota se transferirá a un soporte físico, para que pueda utilizarse como prueba por las autoridades que investiguen el caso (nivel alto).

Sección Quinta
Del registro de actividades

De la operación cotidiana

Artículo 39. El responsable de los SDPS mantendrá estricto control y registro de:

I. Las autorizaciones emitidas para facultar a un servidor público como usuario para interactuar con uno o más SDPS, ya sea que dicho servidor público lo haga acudiendo al área de consulta o desde otro lugar distinto, fuera de dicha área (nivel básico);

II. La asignación, actualización y remplazo de llaves, tarjetas, contraseñas de acceso y demás elementos que entregue a los usuarios, para que éstos puedan activar los mecanismos de apertura de puertas y mobiliario en las zonas de acceso restringido (nivel básico);

III. Las autorizaciones emitidas a los usuarios y demás personal debidamente registrado que soliciten acceso a las áreas de recepción o resguardo. Para ello, el encargado deberá anotar:

a) Quién solicita el acceso,
b) Cuándo solicita el acceso,
c) Cuándo se lleva a cabo el acceso, y
d) La razón que motiva el acceso (nivel básico);

IV. Las autorizaciones emitidas a los usuarios que soliciten permiso para extraer soportes electrónicos que contengan datos personales del área de consulta. Para ello, el encargado deberá anotar:

a) Quién hace la solicitud,
b) Qué documentos se lleva y en qué tipo de soporte (físico o electrónico),
c) Cuándo se los lleva,
d) Cuándo promete devolverlos (si aplica),
e) Cuándo efectivamente los devuelve (si aplica), y
f) Por qué necesita llevárselos (nivel medio);

V. Las autorizaciones emitidas a los usuarios que soliciten permiso para introducir a las zonas de acceso restringido aparatos como los descritos en la sección sexta del capítulo sexto de este título, relativa a "equipo no autorizado". Para ello, el encargado deberá anotar:

a) Quién hace la solicitud,
b) Qué equipo introduce,
c) Cuándo y por cuánto tiempo, y
d) Por qué necesita introducirlo (nivel medio), y

VI. El sistema de videovigilancia remota registrará las actividades diarias y los incidentes en las zonas de acceso restringido (nivel alto).

Sección Sexta
De la divulgación de incidentes

Artículo 40. En caso de que se presente un incidente, se deberá seguir el procedimiento que el Sujeto Obligado tenga definido (nivel básico).

En todo caso, dicho procedimiento deberá incluir las siguientes actividades, sin necesidad de que se realicen en el orden en que aparecen:

I. El responsable del personal de vigilancia deberá emitir un informe al responsable de los SDPS, en un plazo no mayor a 3 días naturales de haber ocurrido el incidente (nivel básico);

II. En caso de robo o extravío de datos personales en soportes electrónicos, el titular del Sujeto Obligado y/o el responsable de los SDPS, al tener conocimiento del incidente, deberá dar vista al órgano interno de control, al área jurídica y/o al servidor público que cuente con facultades para presentar denuncias o querellas de cada Sujeto Obligado, en términos de sus reglamentos interiores o estatutos orgánicos, según corresponda, para que cada uno, en el ámbito de sus atribuciones, determine lo conducente (nivel básico);

III. En un plazo no mayor a 3 días naturales de haber ocurrido el incidente, el responsable de los SDPS deberá dar aviso al público, mediante un desplegado de prensa que difunda dicha circunstancia o hecho por diversos medios, según la gravedad del caso, a escala local, regional, municipal o nacional (nivel medio), y

IV. En caso de robo o extravío de datos personales, se alertará 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 SDPS dará aviso por escrito a dichos titulares, a más tardar 5 días naturales tras haber ocurrido el incidente, recabando el acuse de recibido de esta notificación. Con anticipación a dicho escrito, si se cuenta con los datos actualizados, se dará aviso por correo electrónico o por teléfono (nivel básico).

De la supervisión

Artículo 41. El Comité de información del Sujeto Obligado deberá proponer la realización de una supervisión o verificación interna para las Unidades Administrativas que mantienen y operan SDPS, así como para los terceros contratados que interactúen con dichos SDPS (nivel básico).

Sección Séptima
De la baja de datos personales

De la baja de datos personales

Artículo 42. Para proceder a la baja documental de soportes electrónicos que contengan datos personales, deberán observarse las disposiciones establecidas al respecto para la organización y conservación de los archivos en posesión de los Sujetos Obligados y, según corresponda, lo siguiente:

I. Todo soporte electrónico que sea dado de baja (sea por obsolescencia, sustitución u otra causa) deberá pasar por un proceso de preparación antes de ser desechado. Dicho proceso deberá incluir la transferencia del contenido que sea preciso conservar hacia otro soporte electrónico y la destrucción, inhabilitación o daño que deje inservible dicho soporte (nivel básico);

II. Las únicas personas autorizadas para realizar tal proceso de preparación serán el área de sistemas y el personal de vigilancia (nivel básico);

III. Los métodos de destrucción de soportes electrónicos que contengan datos personales deberán estar definidos en el manual de operaciones de los SDPS o, si no lo están, serán aprobados por el responsable de los SDPS antes de ejecutarlos (nivel básico), y

IV. El encargado de los SDPS deberá:

a) Vigilar que se sigan los procedimientos y se utilicen los mecanismos para asegurar la destrucción de los soportes electrónicos que contengan datos personales (nivel básico), y
b) Llevar una bitácora en la cual se registre la baja de los soportes electrónicos que contengan datos personales, en la que anotará:

   i. Nombre y firma de la persona que realiza la acción,
   ii. Fecha y hora en que se realiza la acción,
   iii. Destino que se dará al soporte electrónico desechado, y
   iv. Nombre y forma (visto bueno) del responsable de los SDPS (nivel básico).

Capítulo Quinto
De las medidas de seguridad para transmisión de datos personales

Sección Primera
De la transmisión de datos personales en soportes físicos

De la transmisión mediante traslado físico

Artículo 43. La transmisión de datos personales mediante traslado físico deberá sujetarse a lo siguiente, según corresponda:

I. La transmisión de datos personales en soportes físicos dentro de las instalaciones del Sujeto Obligado se realizará mediante la vía elegida, de común acuerdo entre las partes: mensajero interno, asistente secretarial o visita personal, entre otras alternativas (nivel básico);

II. La transmisión de datos personales en soportes físicos al exterior se realizará mediante un servicio de mensajería externo. En este caso, se definirá un destinatario primario y otro secundario, por si el mensajero no encuentra al primero (nivel medio);

II. El paquete con soportes físicos que contengan datos personales deberá trasladarse debidamente sellado, de tal manera que sea perceptible cualquier violación o apertura no autorizada (nivel básico);

III. La entrega del paquete se realizará sólo si el destinatario acredita su identidad. Para ello, el destinatario deberá presentar una identificación oficial con fotografía (credencia de elector, pasaporte o documento semejante) y el mensajero deberá recabar el nombre, firma y número de referencia que aparezca en tal identificación, además de la fecha de entrega (nivel medio);

IV. El mensajero no podrá entregar el paquete si el destinatario no acredita su identidad. En este caso, será imperativo que el mensajero devuelva dicho paquete al transmisor (nivel medio), y

V. El responsable de los SDPS deberá verificar que el mensajero entregó el paquete al destinatario. Si el transmisor detecta que dicho paquete se entregó a otra persona, deberá iniciar el proceso de atención de un incidente (nivel medio).

Sección Segunda
De la transmisión de datos personales en soportes electrónicos

De la preparación previa a la transmisión

Artículo 44. El Sujeto Obligado, previo a la transmisión de los datos personales, deberá ajustarse a lo siguiente, según corresponda:

I. Los datos personales que sean enviados a un destinatario autorizado para manipularlos o procesarlos serán sometidos a un proceso de preparación anterior a la transmisión. En tal caso, el encargado que realice dicho proceso deberá:

a) Generar archivos electrónicos que contengan los datos personales solicitados en un formato que permita al destinatario efectuar las operaciones que requiera (nivel básico), y
b) Someter dichos archivos a un proceso de encriptación que los proteja durante su trayecto, mediante la aplicación de un nivel de encriptación alto, no menor a 1024 bits (nivel medio);

II. Los datos personales que sean enviados a un destinatario autorizado para manipularlos o procesarlos no podrán ser reintegrados al SDP del cual fueron extraídos, a menos que el destinatario haya efectuado una corrección solicitada por el titular de los datos (nivel básico), y

III. Los datos personales que sean enviados a un destinatario no autorizado para manipularlos o procesarlos deberán ser sometidos a un proceso distinto de preparación anterior a la transmisión. En este caso, el encargado que realice dicho proceso deberá:

a) Generar archivos electrónicos que contengan los datos personales solicitados en un formato protegido, de manera que el destinatario puede examinar su contenido, pero no pueda editarlo, copiarlo ni imprimirlo (nivel medio), y
b) Someter dichos archivos a un proceso de encriptación que los proteja durante su trayecto, mediante la aplicación de un nivel de encriptación medio, no menor a 512 bits (nivel medio).

De la transmisión mediante traslado físico

Artículo 45. La transmisión mediante traslado físico por parte del Sujeto Obligado deberá sujetarse a lo siguiente, según corresponda:

I. La transmisión de datos personales en soportes electrónicos dentro de las instalaciones del Sujeto Obligado se efectuará mediante la vía elegida, de común acuerdo entre las partes: mensajero interno, asistente secretarial o visita personal, entre otras alternativas (nivel básico);

II. La transmisión de datos personales en soportes electrónicos al exterior se realizará mediante un servicio de mensajería externo. En este caso, se definirán un destinatario primario y otro secundario, por si el mensajero no encuentra al primero (nivel medio);

III. El paquete con soportes electrónicos que contengan datos personales se trasladará debidamente sellado, de tal manera que sea perceptible cualquier violación o apertura no autorizada. Dichos soportes electrónicos contendrán los archivos electrónicos resultantes del proceso de preparación previo a la transmisión (nivel básico);

IV. La entrega del paquete se realizará sólo si el destinatario acredita su identidad. Para ello, éste deberá presentar una identificación oficial con fotografía (credencial de elector, pasaporte o documento semejante) y el mensajero deberá recabar el nombre, firma y número de referencia que aparezca en tal identificación, además de la fecha de entrega (nivel medio);

V. El mensajero no podrá entregar el paquete si el destinatario no acredita su identidad. En este caso, será imperativo que el mensajero devuelva dicho paquete al trasmisor (nivel medio), y

VI. El encargado de los SDPS verificará que el mensajero entregó el paquete al destinatario. Si el transmisor detecta que dicho paquete fue entregado a otra persona, iniciará el proceso de atención de un incidente (nivel medio).

De la transmisión mediante redes de comunicación electrónica

Artículo 46. La transmisión de soportes electrónicos que contengan datos personales previamente preparados para su transmisión podrá realizarse mediante redes de comunicación electrónica (nivel básico).

El transmisor deberá recabar por escrito el acuse de recibido del destinatario, sea por correo electrónico o mediante oficio enviado por fax (nivel medio).

Sección Tercera
De las medidas para la prevención de intrusiones desde el exterior

De la prevención de intrusiones desde el exterior

Artículo 47. El Sujeto Obligado deberá tomar las medidas que se indican a continuación, con el fin de prevenir las intrusiones desde el exterior, según corresponda:

I. Deberán instalarse dispositivos de alta seguridad, en caso de que la red de comunicación electrónica (que conecta los servidores que contienen datos personales con las computadoras que se utilizan para acceder a ellos) esté conectada a internet.

Los referidos dispositivos deberán incluir sistemas de protección perimetral (cortafuegos), de detección de intrusos, de prevención de intrusiones y de análisis de protocolos, además de filtros de contenido;

II. Se aplicarán las medidas necesarias y suficientes para que los puntos de acceso inalámbrico de la red de comunicación electrónica del Sujeto Obligado sean seguros y no tengan huecos que puedan ser aprovechados por intrusos (nivel medio);

III. Se aplicarán las disposiciones establecidas en el capítulo sexto de este título, relativo a "Medidas de seguridad para equipo de cómputo en zonas de acceso restringido" (nivel medio);

IV. El personal de sistemas deberá mantener 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 con los SDPS (nivel medio);

V. Si un equipo de cómputo queda en manos de una persona no autorizada o si es dado de baja, deberá utilizarse la citada memoria técnica para cancelar la configuración del equipo en cuestión (nivel medio), y

VI. El personal de vigilancia o el encargado de los SDPS, en coordinación con el personal de sistemas, realizará, de manera periódica y programada, análisis de vulnerabilidades y pruebas de intrusión controladas en la infraestructura de cómputo, almacenamiento y comunicación. El objeto de esta actividad será aplicar las medidas correctivas necesarias, a fin de cerrar las vulnerabilidades encontradas y evitar posibles incidentes de intrusión (nivel medio).

Sección Cuarta
Del registro de actividades

De la operación cotidiana
Artículo 48. El encargado de los SDPS mantendrá estricto control y registro de:

I. 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 (nivel básico), y

II. Todas las transmisiones efectuadas. Para ello, anotará los datos necesarios para emitir informes sobre la transmisión, según se prevea en las disposiciones aplicables y en estos Lineamientos (nivel básico).

Sección Quinta
De la divulgación de incidentes

Artículo 49. En caso de que se presente un incidente, deberá seguirse el procedimiento que el Sujeto Obligado tenga definido (nivel básico).

En todo caso, dicho procedimiento deberá incluir las siguientes actividades, sin necesidad de que se realicen en el orden en que aparecen:

I. El responsable del personal de vigilancia deberá emitir un informe al responsable de los SDPS, en un plazo no mayor a 3 días naturales de haber ocurrido el incidente (nivel básico);

II. En caso de robo o extravío de datos personales en soportes físicos, el titular del Sujeto Obligado y/o el responsable de los SDPS, al tener conocimiento del incidente, deberá dar vista al órgano interno de control, al área jurídica y/o al servidor público que cuente con las facultades para presentar denuncias o querellas de cada Sujeto Obligado, en términos de sus reglamentos interiores o estatutos orgánicos, según corresponda, para que cada uno, en el ámbito de sus atribuciones, determine lo conducente (nivel básico);

III. En un plazo no mayor a 3 días naturales de haber ocurrido el incidente, el responsable de los SDPS deberá dar aviso al público, mediante un desplegado de prensa que difunda el hecho por diversos medios, según la gravedad del caso, a escala local, regional o nacional (nivel medio), y

IV. En caso de robo o extravío de datos personales, se alertará 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 SDPS avisará por escrito a dichos titulares, a más tardar 5 días naturales tras haber ocurrido el incidente, recabando el acuse de recibo de esta notificación. Con anticipación a dicho escrito, si se cuenta con los datos actualizados, dará aviso por correo electrónico o por teléfono (nivel básico).

De la supervisión
Artículo 50. El Comité de Información del Sujeto Obligado deberá proponer la realización de una supervisión a las Unidades Administrativas que mantienen y operan SDPS, así como a los terceros contratados (nivel básico).

Capítulo Sexto
De las medidas de seguridad para equipo de cómputo en zonas de acceso restringido

Sección Primera
De las computadoras de escritorio

De la recepción de equipo de cómputo

Artículo 51. Las MS para la recepción de computadoras de escritorio asignadas para las zonas de acceso restringido consistirán en lo siguiente, según corresponda:

I. Cada computadora de escritorio asignada para las zonas de acceso restringido, sea nueva o usada, deberá pasar por un proceso de preparación inicial, a fin de instalarle sólo software autorizado, configurado para brindar mayor seguridad que la predeterminada por el fabricante (nivel básico);

II. El proceso de preparación inicial de cada computadora de escritorio incluirá, antes de instalar dicho software, sobrescribir con un único valor (uno o cero) el 100% del medio principal de almacenamiento no volátil, mediante alguna herramienta especializada para ello (nivel medio);

III. El área de sistemas de cada Sujeto Obligado deberá preparar y actualizar la lista de software actualizado para computadoras de escritorio asignadas para las zonas de acceso restringido. Este documento se realizará en coordinación con el responsable de los SDPS, según las necesidades y funciones que desempeñe el personal autorizado a su cargo (nivel medio);

IV. Las únicas personas autorizadas para realizar el proceso de preparación inicial serán los integrantes de las áreas de sistemas o de vigilancia (nivel medio);

V. El encargado de los SDPS supervisará y verificará que cada computadora de escritorio cumpla los requerimientos de instalación establecidos y las configuraciones de seguridad definidas (nivel básico), y

VI. El proceso de preparación inicial de cada computadora de escritorio se registrará en un formulario, que será archivado por el área de sistemas o de vigilancia (nivel básico).

Del resguardo de equipo de cómputo

Artículo 52. Cada computadora de escritorio asignada para las zonas de acceso restringido deberá estar asegurada físicamente, para evitar el robo del gabinete o la sustracción de piezas o partes. Para ello, estará resguardada con cajones de protección, candados o cualquier otro dispositivo que impida la manipulación del gabinete y el acceso físico al interior del equipo (nivel básico).

De la operación de equipo de cómputo

Artículo 53. La operación de las MS en las computadoras de escritorio asignadas para las zonas de acceso restringido deberá sujetarse a lo siguiente, según corresponda:

I. Los puertos de comunicación que no se utilicen (USB, paralelo, serial, etcétera) permanecerán deshabilitados (en el interior del equipo) o cancelados (en el exterior). Los cables o dispositivos conectados a los puertos que sí se utilicen estarán asegurados, para evitar su desconexión. Las cancelaciones podrán ser abiertas por personal autorizado del área de sistemas (nivel medio);

II. Los dispositivos de almacenamiento removible (unidades de disco flexible, quemadores de CD/DVD, etcétera) estarán deshabilitados (en el interior del equipo) o cancelados (en el exterior). Las cancelaciones podrán ser abiertas por personal autorizado del área de sistemas (nivel medio);

III. Los dispositivos de conexión inalámbrica (Wi-Fi, Bluetooth, infrarrojo, etcétera) no existirán en estas computadoras (nivel medio), y

IV. El acceso a una computadora de escritorio dentro de una zona de acceso restringido, a fin de realizar labores de soporte técnico o mantenimiento preventivo y correctivo, se dará exclusivamente al personal autorizado del área de sistemas o a un proveedor externo subcontratado. En cualquier caso, el responsable de los SDPS deberá autorizar, supervisar y registrar el acceso, archivando la autorización que emita (nivel básico).

De la atención de fallas

Artículo 54. Cuando se presente una falla en una computadora de escritorio asignada para las zonas de acceso restringido, deberá realizarse lo siguiente, según corresponda:

I. El usuario del equipo o, en su caso, el responsable de los SDPS, deberá reportar el caso de inmediato al área de sistemas y, de ser posible, tomar las primeras acciones para evitar un mayor deterioro del equipo, siguiendo las indicaciones que reciba del personal del área de sistemas (nivel básico), y

II. En caso de que la falla requiera que la computadora de escritorio sea retirada de la zona de acceso restringido para su reparación, los medios de almacenamiento no volátil serán extraídos y puestos bajo resguardo, a fin de evitar la pérdida, robo o daño de los datos personales almacenados en ellos. Tal operación será realizada por el personal autorizado del área de sistemas (nivel básico).

De la baja de equipo de cómputo

Artículo 55. Toda computadora de escritorio asignada para las zonas de acceso restringido que sea dada de baja (sea por obsolescencia, sustitución u otra causa) deberá sujetarse a lo siguiente:

I. Deberá pasar por un proceso de preparación final (nivel básico);

II. El proceso de preparación final implicará transferir a otro equipo los documentos que contengan información que sea preciso conservar y sobrescribir con un único valor (uno o cero) el 100% de los medios de almacenamiento no volátil, mediante alguna herramienta especializada para ello (nivel básico);

III. Las únicas personas autorizadas para realizar el proceso de preparación final serán los integrantes del área de sistemas y de vigilancia (nivel básico), y

IV. El proceso de preparación final deberá quedar registrado en un formulario, que será archivado por el área de sistemas o el personal de vigilancia, con el formulario que, en su momento, registró el proceso de preparación inicial del equipo (nivel básico).

Sección Segunda
De los servidores

De la recepción de servidor

Artículo 56. Las MS para la recepción de un servidor asignado para las zonas de acceso restringido, sea nuevo o usado, se sujetará a lo siguiente, según corresponda:

I. El servidor asignado para las zonas de acceso restringido deberá pasar por un proceso de preparación inicial, a fin de instalarle el software autorizado, configurado para brindar mayor seguridad que la predeterminada por el fabricante (nivel básico);

II. El proceso de preparación inicial de dicho servidor incluirá, además de la instalación del software, sobrescribir con un único valor (uno o cero) el 100% de los medios principales de almacenamiento no volátil, mediante una herramienta especializada para ello (nivel básico);

III. El área de sistemas del Sujeto Obligado, en coordinación con el responsable de los SDPS, deberá preparar y actualizar la lista de software autorizado para los servidores asignados para las zonas de acceso restringido, según las necesidades y funciones que desempeña el personal autorizado a su cargo (nivel básico);

IV. Las únicas personas autorizadas para realizar el proceso de preparación inicial serán los integrantes de las áreas de sistemas o de vigilancia (nivel básico);

V. El encargado de los SDPS supervisará y verificará que el servidor cumpla los requerimientos de instalación establecidos y las configuraciones de seguridad definidas (nivel básico), y

VI. El proceso de preparación inicial de un servidor asignado para las zonas de acceso restringido quedará registrado en un formulario, que deberá ser archivado por el área de sistemas o de vigilancia (nivel básico).

Del resguardo de servidor

Artículo 57. Todo servidor que se encuentre bajo la custodia del área de sistemas deberá instalarse en un lugar que facilite adoptar lo siguiente:

I. Medidas de seguridad: Acceso restringido y sistema de videovigilancia remota;

II. Medidas para su funcionamiento: Temperatura de operación adecuada; mantenimiento preventivo y correctivo, y atención inmediata en caso de fallas;

III. Medidas para su operación continua: Elaboración y restauración de respaldos y sustitución rápida de partes dañadas (nivel básico), y

IV. Aquel servidor que no se encuentre bajo la custodia del área de sistemas deberá estar asegurado físicamente, para evitar el robo del gabinete o la sustracción de piezas o partes. Para tal propósito, estará resguardado mediante cajones de protección, candados o cualquier otro dispositivo que impida la manipulación del gabinete y el acceso físico al interior del equipo (nivel básico).

De la operación de servidores asignados

Artículo 58. La operación de servidores asignados para las zonas de acceso restringido, sean nuevos o usados, deberá sujetarse a lo siguiente, según corresponda:

I. Aquel servidor que no se encuentre bajo la custodia del área de sistemas tendrá deshabilitados (en el interior de equipo) o cancelados (en el exterior) los puertos de comunicación (USB, paralelo, serial, etcétera) que no se utilicen. Los cables o dispositivos conectados a los puertos que sí se utilicen estarán asegurados, para evitar su desconexión. Las cancelaciones podrán ser abiertas por el personal de sistemas (nivel básico);

II. Aquel servidor que no se encuentre bajo la custodia del área de sistemas tendrá deshabilitados (en el interior del equipo) o cancelados (en el exterior) los dispositivos de almacenamiento removible (unidades de disco flexible, quemadores de CD/DVD, etcétera). Las cancelaciones podrán ser abiertas por el personal de sistemas (nivel básico);

III. Ni en los servidores asignados para las zonas de acceso restringido ni en aquéllos que se encuentren bajo la custodia del área de sistemas, existirán dispositivos de conexión inalámbrica (Wi-Fi, Bluetooth, infrarrojo, entre otros) (nivel básico), y

IV. El acceso a un servidor que no se encuentre bajo la custodia del área de sistemas, a fin de realizar labores de soporte técnico o mantenimiento preventivo y correctivo, será exclusivamente para el personal del área de sistemas o un proveedor externo subcontratado. En cualquier caso, el encargado de los SDPS autorizará, supervisará y registrará el acceso, archivando la autorización que emita (nivel básico).

De la atención de fallas

Artículo 59. Cuando se presente una falla en un servidor, se deberá sujetar a lo siguiente:

I. Cuando la falla se presente en un servidor que no se encuentre bajo la custodia del área de sistemas, el responsable de los SDPS deberá reportarla de inmediato al área de sistemas y, de ser posible, tomará las primeras acciones, para evitar un mayor deterioro del equipo, siguiendo las indicaciones que reciba del personal del área de sistemas (nivel básico);

II. Para los servidores críticos que se encuentren bajo la custodia del área de sistema, tal área deberá tener contratada una póliza de reparación y mantenimiento preventivo y correctivo, cuyo tiempo de respuesta sea suficiente para atender la criticidad de la información contenida en el equipo (nivel básico), y

III. 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 serán extraídos y puestos bajo resguardo, para evitar la pérdida, robo o daño de los datos personales almacenados en él. Tal operación será realizada por el personal autorizado del área de sistemas (nivel básico).

De la baja de equipo de cómputo

Artículo 60. Todo servidor que sea dado de baja (sea por obsolescencia, sustitución u otra causa), se sujetará a lo siguiente, según corresponda:

I. Deberá pasar por un proceso de preparación final (nivel básico);

II. El proceso de preparación final implicará transferir a otro equipo los documentos que contengan información que sea preciso conservar y sobrescribir con un único valor (uno o cero) el 100% de los medios de almacenamiento no volátil, mediante alguna herramienta especializada para ello (nivel básico);

III. Las únicas personas autorizadas para realizar el proceso de preparación final serán los integrantes de las áreas de sistema y de vigilancia (nivel básico), y

IV. El proceso de preparación final de un servidor deberá quedar registrado en un formulario, que será archivado por el área de sistemas o de vigilancia, con el formulario que, en su momento, registró el proceso de preparación inicial del equipo (nivel básico).

Sección Tercera
De las impresoras y otros equipos periféricos autorizados

De la recepción de equipo de cómputo periférico

Artículo 61. Las MS para la recepción de impresoras y equipos periféricos autorizados (monitores, pantallas planas, etcétera) asignados para las zonas de acceso restringido, sean nuevos o usados, deberán sujetarse a lo siguiente, según corresponda:

I. Los equipos deberán pasar por un proceso de preparación inicial. Con ello, se buscará la presencia de puertos de comunicación (USB, paralelo, red local, etcétera) adicionales al principal, que pudieran utilizarse para conectar dispositivos como los descritos en la sección sexta del capítulo sexto de este título, relativa a "equipo no autorizado" (nivel medio);

II. Los puertos adicionales antes referidos serán inhabilitados (en el interior de equipo) o cancelados (en el exterior), mientras que los cables conectados a los puertos principales quedarán asegurados, para evitar su desconexión. Las cancelaciones podrán ser abiertas por el personal autorizado del área de sistemas (nivel medio);

III. Las únicas personas autorizadas para realizar el proceso de preparación inicial serán los integrantes de las áreas de sistemas y de vigilancia (nivel medio);

IV. El encargado de los SDPS deberá supervisar y verificar que el equipo de cómputo cumpla los requerimientos de instalación establecidos y las configuraciones de seguridad definidas (nivel medio), y

V. El proceso de preparación inicial de una impresora o de un equipo periférico autorizado para las zonas de acceso restringido deberá quedar registrado en un formulario, que será archivado por el área de sistemas o de vigilancia (nivel medio).

Del resguardo de equipo de impresión
Artículo 62. El equipo de impresión deberá estar asegurado físicamente, para evitar el robo o la sustracción de cartuchos de tinta, piezas o partes. Para tal propósito, estará resguardado mediante cajones de protección, candados o cualquier otro dispositivo que impida la manipulación del equipo y el acceso físico a su interior (nivel medio).

El equipo de almacenamiento removible externo deberá mantenerse bajo custodia del área de sistemas o de vigilancia (nivel medio).

De la operación de equipos periféricos
Artículo 63. El uso de impresoras y equipo periférico autorizado que se conecte directamente a computadoras de escritorio y servidores asignados para las zonas de acceso restringido será vigilado, supervisado y, en su caso, autorizado por el responsable de los SDPS (nivel medio).

Las únicas personas autorizadas para utilizar el equipo de almacenamiento removible externo serán los integrantes de las áreas de sistemas y de vigilancia (nivel medio).

De la atención de fallas
Artículo 64. Cuando se presente una falla en una impresora o en un equipo periférico autorizado, se deberá observar lo siguiente:

I. El usuario del equipo o, en su caso, el responsable de los SDPS deberá reportar la falla de inmediato al área de sistemas y, si es posible, tomar las primeras acciones para evitar un mayor deterioro del equipo, siguiendo las indicaciones que reciba del personal del área de sistemas (nivel básico), y

II. En caso de que la falla requiera que la impresora o el equipo periférico autorizado sea retirado de las zonas de acceso restringido para su reparación, si éstos tienen medios de almacenamiento no volátil, deberán ser extraídos y puestos bajo resguardo, para evitar la pérdida, robo o daño de los datos personales almacenados en ellos. Dicha operación será realizada por el personal autorizado del área de sistemas (nivel básico).

De la baja de equipo periférico
Artículo 65. Toda impresora y equipo periférico autorizado que sea dado de baja (sea por obsolescencia, sustitución u otra causa), se sujetará a lo siguiente, según corresponda:

I. Deberán pasar por un proceso de preparación final (nivel básico);

II. Las impresoras y los equipos periféricos autorizados que contengan uno o más medios de almacenamiento no volátil, fijos o removibles, deberán recibir atención especial. En tal caso, el proceso de preparación final implicará transferir a otro equipo los documentos que contengan información que sea preciso conservar y sobrescribir con un único valor (uno o cero) el 100% de los medios de almacenamiento no volátil, mediante una herramienta especializada para ello (nivel medio);

III. Las únicas personas autorizadas para realizar el proceso de preparación final serán los integrantes de las áreas de sistemas y de vigilancia (nivel medio), y

IV. El proceso de preparación final de una impresora o de un equipo periférico autorizado deberá quedar registrado en un formulario, que será archivado por el área de sistemas o de vigilancia, junto al formulario que, en su momento, registró el proceso de preparación inicial del equipo (nivel básico).

Sección Cuarta
Del registro de actividades e inventario

Del control de activos (inventario)
Artículo 66. El área de sistemas deberá llevar un inventario actualizado, independiente de aquél que lleva el área administrativa correspondiente, para todos los activos de cómputo, separados por tipo; o sea, computadoras personales, servidores, impresoras y equipos periféricos autorizados (nivel básico).

De la operación cotidiana
Artículo 67. El responsable de los SDPS mantendrá estricto control y registro de:

I. Las autorizaciones emitidas al personal del área de sistemas o a proveedores externos subcontratados que proporcionen servicios de soporte técnico y mantenimiento preventivo y correctivo para computadoras personales, servidores, impresoras y

equipos periféricos asignados para las zonas de acceso restringido deberán ser registradas por el encargado de los SDPS e incluirán, por lo menos, lo siguiente:

a) Causa que motiva el servicio,
b) Número o identificación de activo del equipo,
c) Fecha y hora, tanto de inicio como de terminación del servicio,
d) Nombre completo y firma de las personas que proporcionan el servicio,
e) Tipo de identificación oficial que utilizan dichas personas para acreditarse (credencial de elector, pasaporte o documento semejante) y número de referencia que aparezca en dicha identificación,
f) Nombre y firma (visto bueno) del responsable de los SDPS que autoriza el acceso, y
g) De manera opcional, fotografía de las personas que obtienen el acceso (nivel básico);

II. Las autorizaciones para la operación de equipo de almacenamiento removible externo por parte del personal de sistemas o de vigilancia, cuando sea necesario llevar a cabo respaldos de la información contenida en los equipos que no se encuentren bajo custodia del área de sistemas (nivel básico), y

III. Las autorizaciones para el uso temporal de dispositivos como los citados en la sección sexta del capítulo sexto de este título, relativa a "equipo no autorizado" que se otorguen al personal autorizado que lo solicite. Dicho registro deberá incluir, al menos, lo siguiente:

a) Causa que motiva la solicitud,
b) Nombre completo de quien solicita la autorización,
c) Fecha en que obtuvo la autorización para interactuar con uno o más SDPS, nombre del responsable de los SDPS que otorgó la autorización y fotocopia del documento que le otorgó la categoría de personal autorizado,
d) Tipo de identificación oficial que utilizan dichas personas para acreditarse (credencial de elector, pasaporte o documento semejante) y número de referencia que aparezca en dicha identificación,
e) Nombre y firma (visto bueno) del responsable de los SDPS que autoriza el acceso,
f) De manera opcional, fotografía de la persona que obtiene el acceso y del equipo no autorizado que utilizará en las zonas de acceso restringido, y
g) Carta responsiva emitida por el usuario, encargado o demás personal, con firma autógrafa y manifiesto en que asuma la responsabilidad por el daño, pérdida o robo de datos personales almacenados en el equipo no autorizado que utilice temporalmente en cualquiera de las zonas de acceso restringido (nivel básico).

IV. El área de sistemas o el personal de vigilancia mantendrán estricto control y registro de:

a) El formulario en que se asienten los detalles del proceso de preparación inicial de cada computadora de escritorio y cada servidor asignado para las zonas de acceso restringido. Dicho registro incluirá, por lo menos, los siguientes datos:

   i. Nombre y firma de las personas que realizan el proceso de preparación inicial,
   ii. Fecha y hora en que se realiza dicho proceso, tanto de inicio como de terminación,
   iii. 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,
   iv. Nombre y firma (visto bueno) del responsable de los SDPS,
   v. Número o identificación de activo del equipo,
   vi. Fecha en que el equipo queda instalado y se pone en operación, y
   vii. Área en la cual queda instalado el equipo (nivel básico);

b) El formulario en que se asienten los detalles del proceso de preparación inicial de cada impresora y cada equipo periférico asignado para las zonas de acceso restringido. Dicho registro incluirá, por lo menos, los siguientes datos:

   i. Nombre y firma de las personas que realizan el proceso de preparación inicial,
   ii. Fecha y hora en que se realiza dicho proceso, tanto de inicio como de terminación,
   iii. 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,
   iv. Nombre y firma (visto bueno) del responsable de los SDPS,
   v. Número o identificación de activo del equipo,
   vi. Fecha en que el equipo queda instalado y se pone en operación, y
   vii. Área en la cual queda instalado el equipo (nivel medio);

c) El inventario actualizado de activos de cómputo, que comprenderá, al menos, los siguientes datos:

i. Descripción,
ii. Área en la cual se instaló el equipo,
iii. Número o identificación de activo que tenía asignado el equipo,
iv. Características del equipo (marca, modelo y número de serie),
v. 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,
vi. 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,
vii. Memoria técnica de las configuraciones de red del equipo, si aplica,
viii. Folio del formulario que registra los detalles del proceso de preparación inicial y fecha de alta en el inventario, y
ix. Folio del formulario que registra los detalles del proceso de preparación final y fecha de baja del inventario (nivel básico);

d) El formulario en el cual se asienten los detalles del proceso de preparación final de cada computadora de escritorio y cada servidor asignado para las zonas de acceso restringido. Dicho registro incluirá, por lo menos, los siguientes datos:

i. Área en la cual estaba instalado el equipo,
ii. Número o identificación de activo que tenía asignado el equipo,
iii. Nombre y firma de la persona que realiza el proceso de preparación final,
iv. Fecha y hora en que se realiza dicho proceso, tanto de inicio como de terminación,
v. 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,
vi. Destino que se dará al equipo dado de baja,
vii. Fecha en que el equipo es efectivamente dado de baja, y
viii. Nombre y firma (visto bueno) del responsable de los SDPS (nivel básico);

e) El formulario en cual se asienten los resultados del proceso de preparación final de cada impresora y cada equipo periférico asignado para las zonas de acceso restringido. Dicho registro incluirá, por lo menos, los siguientes datos:

i. Área en la cual estaba instalado el equipo,
ii. Número o identificación de activo que tenía asignado el equipo,
iii. Nombre y firma de la persona que realiza el proceso de preparación final,
iv. Fecha y hora en que se realiza dicho proceso, tanto de inicio como de terminación,
v. 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,
vi. Destino que se dará al equipo dado de baja,
vii. Fecha en que el equipo es efectivamente dado de baja, y
viii. Nombre y firma (visto bueno) del responsable de los SDPS (nivel medio), y

f) El formulario en cual se registren los incidentes, que deberá contener la siguiente información:

i. Registro del incidente, con las siguientes especificaciones: tipo, gravedad, impacto, persona que lo detectó y personal que fue notificado,
ii. Procedimientos implementados para recuperar los datos o procesos seguidos para la pronta restauración de la operación del sistema, y
iii. Seguimiento en el cual se indique el personal que intervino en la atención del incidente, metodología aplicada, datos recuperados y, en su caso, datos que ha sido necesario grabar manualmente en el proceso de recuperación (nivel básico).

Sección Quinta
De la divulgación de incidentes

De la presentación de incidentes

Artículo 68. En caso de que se presente un incidente, se seguirá el procedimiento que el Sujeto Obligado tenga establecido y conforme a estos Lineamientos (nivel básico).

En todo caso, dicho procedimiento deberá incluir las siguientes actividades, sin necesidad de que se realicen en el orden en que aparecen:

I. El responsable del personal de vigilancia emitirá un informe al responsable de los SDPS, en un plazo no mayor a 3 días naturales después de haber ocurrido el incidente (nivel básico);

II. En caso de robo o extravío de datos personales en soportes físicos, el titular del Sujeto Obligado o el responsable de los SDPS, al tener conocimiento del incidente, dará vista al órgano interno de control, al área jurídica y/o al servidor público que cuente con facultades para presentar denuncias o querellas de cada Sujeto Obligado, en términos de sus reglamentos interiores o estatutos orgánicos, según corresponda, para que cada uno, en el ámbito de sus atribuciones, determine lo conducente (nivel básico);

III. En un plazo no mayor a 3 días naturales de haber ocurrido el incidente, el responsable de los SDPS dará aviso al público mediante un desplegado de prensa que difunda el hecho por diversos medios, según la gravedad del caso, a escala local, regional o nacional (nivel medio), y

IV. En caso de robo o extravío de datos personales, se alertará 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 SDPS dará aviso por escrito a dichos titulares, a más tardar 5 días naturales tras haber ocurrido el incidente, recabando el acuse de recibo de esta notificación. Con anticipación a dicho escrito, si se cuenta con los datos actualizados, se dará aviso por correo electrónico o por teléfono (nivel básico).

De la supervisión de unidades administrativas.
Artículo 69. El Comité de Información del Sujeto Obligado deberá proponer la realización de una supervisión interna para las Unidades Administrativas que mantienen y operan SDPS, así como a los terceros contratados (nivel básico).

Sección Sexta
Del equipo no autorizado

De las computadoras portátiles
Artículo 70. Respecto de las computadoras portátiles, se observará lo siguiente, según corresponda:

I. No estará permitido el libre acceso de computadoras portátiles a las zonas de acceso restringido (nivel básico);

II. Será posible autorizar el acceso temporal de computadoras portátiles, de conformidad con las disposiciones descritas en el capítulo quinto de este título, relativo a "operación cotidiana" de la sección cuarta de "registro de actividades e inventario" (nivel básico);

III. En caso de que se autorice el acceso temporal de una computadora portátil, el área de sistemas o el personal de vigilancia llevará a cabo una revisión inicial del equipo, la cual incluirá:

a) La revisión y el registro de la estructura de los medios de almacenamiento no volátil; específicamente, el número de particiones y el espacio libre,
b) La detección de cualquier software que suponga un riesgo, ya sea por pérdida de datos personales o por sustracción, como malware y herramientas de intrusión, y
c) La inhabilitación de dispositivos de conexión inalámbrica que supongan un riesgo de extracción de datos personales por una persona que se encuentre fuera de las zonas de acceso restringido (nivel medio);

IV. En caso de que sea necesario el traslado de datos personales al equipo no autorizado, éste se realizará con las siguientes restricciones: sólo para lectura, no para modificación, sustracción, impresión o quemado (nivel medio);

V. Al finalizar la visita, se efectuará una revisión final de la computadora portátil por parte del área de sistemas o del personal de vigilancia, que incluirá:

a) La revisión y el registro de la estructura de los medios de almacenamiento no volátil, con el propósito de comprobar que el número de particiones y el espacio libre siga siendo el mismo que en la revisión inicial, para detectar si hay archivos almacenados en el equipo portátil que no estaban al inicio, y
b) Las áreas no utilizadas (vacías) en los medios de almacenamiento no volátil se sobrescribirán con un único valor (uno o cero), mediante una herramienta especializada para ello (nivel básico), y

VI. Por el riesgo que implica, estará 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, como se dispone en el capítulo quinto de este título, relativo a "Medidas de seguridad para transmisión de datos personales" (nivel medio).

De los dispositivos de almacenamiento externo
Artículo 71. Respecto de los dispositivos de almacenamiento externo, se deberá observar lo siguiente, según corresponda:

I. Sin excepción alguna, no se permitirá el acceso de dispositivos de almacenamiento externo ajenos a la institución o sin autorización (nivel básico);

II. Será posible autorizar el acceso temporal de dispositivos de almacenamiento externo, de conformidad con las disposiciones descritas en el capítulo quinto de este título, relativo a "operación cotidiana" de la sección cuarta de "registro de actividades e inventario" (nivel básico);

III. En caso de que se autorice el acceso temporal de dispositivos de almacenamiento externo, el área de sistemas o el personal de vigilancia llevará a cabo una revisión inicial del equipo, que incluirá:

a) La revisión y el registro de la estructura de los medios de almacenamiento no volátil; específicamente, el número de particiones y el espacio libre,
b) La detección de cualquier software que suponga un riesgo, ya sea por pérdida de datos personales o por sustracción, como malware y herramientas de intrusión, y
c) La inhabilitación de dispositivos de conexión inalámbrica que supongan un riesgo de extracción de datos personales por una persona que se encuentre fuera de las zonas de acceso restringido (nivel medio);

IV. En caso de que sea necesario el traslado de datos personales al equipo no autorizado, éste se realizará con las siguientes restricciones: sólo para lectura, no para modificación, sustracción, impresión ni quemado (nivel medio);

V. 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, que incluirá:

a) La revisión y el registro de la estructura de los medios de almacenamiento no volátil, para comprobar que el número de particiones y el espacio libre siga siendo el mismo que en la revisión inicial, lo que permitiría detectar si hay archivos almacenados en el equipo portátil que no estaban al inicio, y
b) Las áreas no utilizadas (vacías) en los medios de almacenamiento no volátil se sobrescribirán con un único valor (uno o cero), mediante una herramienta especializada para ello (nivel medio), y

VI. Por el riesgo que implica, estará 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, como se describe en el capítulo quinto de este título, relativo a "Medidas de seguridad para transmisión de datos personales" (nivel medio).

De otros dispositivos no autorizados
Artículo 72. Respecto de otros dispositivos no autorizados, se observará lo siguiente, según corresponda:

I. Sin excepción alguna, no se permitirá el acceso de dispositivos portátiles de almacenamiento externo (memoria USB, reproductor MP3, teléfono celular, etcétera) ajenos a la institución (nivel básico);

II. Será posible autorizar el acceso temporal de estos dispositivos, de conformidad con las disposiciones descritas en el capítulo quinto de este título, relativo a "Operación cotidiana" de la sección cuarta de "Registro de actividades e inventario" (nivel básico);

III. Por el riesgo que implica, estará 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, como se describe en el capítulo quinto de este título, relativo a "Medidas de seguridad para transmisión de datos personales" (nivel básico), y

IV. Estará prohibida la introducción de objetos que puedan dañar o alterar los soportes físicos y electrónicos que contengan datos personales, como tijeras, navajas, marcadores, alimentos y bebidas, entre otros (nivel básico).

Capítulo Séptimo
De las medidas de seguridad para asegurar continuidad y enfrentar desastres

Sección Primera
Del respaldo y recuperación de sistemas de datos personales automatizados

De los medios de almacenamiento autorizados y no autorizados
Artículo 73. Los medios de almacenamiento no volátil autorizados para la generación y almacenamiento de copias de seguridad o respaldos se dividirán en dos grupos: fijos y removibles. Los medios fijos son los discos duros internos. Los medios removibles pueden ser magnéticos (cintas y discos duros externos); ópticos (CD y DVD), o magneto-ópticos (discos magneto-ópticos) (nivel básico).

Los medios de almacenamiento no volátil autorizados se utilizarán solos o combinados, según las necesidades de respaldo y de restauración, para garantizar la operación continua de los SDPS (nivel básico).

El uso de las unidades para lectura y escritura de tales medios autorizados será exclusivo para el área de sistemas, que se encargará 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, existe, cuando menos, una forma de restringir el uso de dicho puerto (nivel básico).

Todos aquellos medios de almacenamiento, así como sus respectivas unidades para lectura y escritura, que no entren en las descripciones anteriores, serán considerados como 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. Algunos ejemplos son los memory sticks, agendas digitales, teléfonos celulares inteligentes, cámaras digitales de instantáneas fijas o video y dispositivos portátiles para reproducción de música y video, como el Apple iPod y similares (nivel básico).

El encargado de los SDPS, en colaboración con el personal de seguridad, deberá implementar medidas para restringir el acceso y uso de los dispositivos no autorizados. Los puntos de revisión y el sistema de videovigilancia remota coadyuvarán a este fin (nivel básico).

Del inventario y clasificación de medios

Artículo 74. El inventario y clasificación de medios de los SDPS por parte del Sujeto Obligado deberá sujetarse a lo siguiente:

I. La existencia de un inventario de los equipos autorizados para almacenar información crítica, así como de aquéllos que se utilicen para generar copias de seguridad de la información (nivel básico);

II. Los medios de almacenamiento no volátil que contengan las copias de seguridad mencionadas deberán ser clasificados y protegidos por el área de sistemas o el personal de vigilancia, a fin de evitar su extravío, robo o daño accidental (nivel básico), y

III. Se deberán seguir los procedimientos archivísticos necesarios y suficientes para clasificar los medios de almacenamiento no volátil, ya sean magnéticos, ópticos o magneto-ópticos, dependiendo de las tecnologías utilizadas; en caso de que existan dos o más tecnologías, se llevará un control por cada una. El propósito deberá ser reducir el tiempo de espera para localizar los archivos que sea necesario restaurar (nivel básico).

Del almacenamiento de respaldos

Artículo 75. El almacenamiento de respaldos de los SDPS por parte del Sujeto Obligado se sujetará a lo siguiente:

I. El almacenamiento de los respaldos (es decir, de los medios de almacenamiento removibles que los contengan) deberá realizarse en lugares seguros; preferentemente, en bóvedas de seguridad (nivel medio);

II. El remplazo de dichos medios de almacenamiento se deberá llevar a cabo mediante un esquema calendarizado. Por ejemplo, un esquema de remplazo mínimo incluirá realizar un respaldo general cada 7 días y se almacenará durante un mes, antes de remplazarlo nuevamente. En la bóveda, quedarán siempre cuatro semanas de respaldo (nivel medio);

III. Los respaldos se llevarán a cabo a diario, de modo incremental y en línea, en caso de que el sistema lo permita. El séptimo día se realizará un respaldo general, fuera de línea, el cual será llevado, como lo dicta el punto anterior, a un lugar seguro para su resguardo (nivel básico), y

IV. Deberá llevarse un registro de las veces que un respaldo se introduce en o se extrae de las bóvedas. Deberán ser sólo dos o, cuando mucho, tres personas quienes estén autorizadas para realizar dichos trámites (nivel medio).

Sección Segunda
De la operación continua de sistemas de datos personales automatizados

De los sitios alternos y restauración

Artículo 76. Con el fin de asegurar la operación continua de los SDPS automatizados, se deberá observar lo siguiente:

I. Deberá existir un sitio alterno para restablecer la operación de un SDP automatizado, en el menor tiempo posible, en caso de un desastre. Para ello, se deberá tener establecido solamente uno de los siguientes tres tipos de sitios:

a) **Sitio alterno frío:** En este tipo de sitios alternos no deberá incluirse 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 y piso falso, entre otros factores,
b) **Sitio alterno tibio:** En este tipo de sitios alternos el equipo deberá estar disponible unas cuantas horas después de ocurrido el desastre, pero no deberá contener datos personales ni software, o
c) **Sitio alterno caliente:** En este tipo de sitios alternos se mantendrán disponibles tanto el equipo como el software y los datos personales, en cualquier momento, y sólo será necesario "dar la orden" para activarlo y hacer posible su operación, en un tiempo mucho más corto que en los sitios alternos anteriores (nivel básico), y

II. Según la criticidad de un SDP automatizado, el manual de operaciones deberá tener definido el tiempo requerido para su restauración como sigue:

a) **No esencial:** Se deberá restaurar en 30 días naturales,
b) **Normal:** Se deberá restaurar en 7 días naturales,
c) **Importante:** Se deberá restaurar en 72 horas,
d) **Urgente:** Se deberá restaurar en 24 horas, o
e) **Crítica o esencial:** Se deberá restaurar entre 1 y 4 horas.

Estos tiempos darán la pauta para elegir el sitio alterno por utilizar (nivel básico).

Del plan de contingencias

Artículo 77. El Sujeto Obligado deberá prever la existencia de un plan de contingencias que documente los procedimientos para restablecer la operación de los sistemas de redes en un sitio alterno que esté separado del centro principal, fuera de las instalaciones del Sujeto Obligado, en otra ciudad, a kilómetros de distancia (nivel básico).

A fin de tener identificados los mínimos requeridos para continuar con la operación, dicho plan de contingencias estará basado en:

I. Un análisis para determinar los requerimientos de soporte de una red; o sea, de equipo, periféricos, cableado y otros semejantes, y

II. Un análisis para identificar el tipo de comunicaciones, como los enlaces requeridos, líneas telefónicas y servicios de redes de comunicación electrónica, tanto del área local como del área ampliada (nivel básico).

Del personal para emergencias

Artículo 78. Dentro del plan de contingencias se deberá identificar al personal que llevará la operación de un SDP automatizado, el cual deberá contar con la capacitación necesaria para seguir los procedimientos de restauración en caso de desastre.

Tales personas deberán estar involucradas en la creación de la documentación necesaria para el mencionado plan (nivel básico).

En dicho plan se deberá designar al personal necesario de cada área, a fin de efectuar la operación y administración de los SDPS automatizados que se restaurarán en el sitio alterno (nivel básico).

Sección Tercera
Del registro de actividades

De las pruebas y simulacros

Artículo 79. El Sujeto Obligado deberá llevar a cabo pruebas y simulacros para disminuir riesgos, en caso de que se presente alguna eventualidad adversa y para comprobar que los sistemas de seguridad y prevención funcionen correctamente y en el tiempo estimado como óptimo. Estas tareas se sujetarán a lo siguiente:

I. Deberá realizarlas el responsable de los SDPS, en coordinación con el área de sistemas y el personal de vigilancia;

II. Deberán realizarse periódicamente, según el nivel de criticidad de la información (nivel básico);

III. Deberá existir un registro de pruebas y simulacros que contenga, cuando menos, los siguientes datos:

a) Fecha y hora, tanto de inicio como de terminación,
b) Nombre de la persona encargada de realizarlas,
c) Nombre de la persona encargada de evaluarlas,
d) Tiempo de restauración,
e) Firma (visto bueno) de los responsables,
f) Observaciones, y
g) Sugerencias de mejora, y

IV. El propósito de este registro será permitir su análisis y evaluación, a fin de realizar las adecuaciones necesarias antes de que se presente una contingencia (nivel básico).

Sección Cuarta
De la divulgación de incidentes

De la incidencia pérdida de información

Artículo 80. En caso de que el incidente se refiera a la pérdida de información provocada por fallas en el equipo o en sus dispositivos de almacenamiento, sea por problemas en instalaciones, acontecimientos de casos fortuitos o de fuerza mayor (desastres naturales, incendios, huelgas, etcétera), se deberá proceder a la declaración de éste. Al momento, deberá ponerse en

marcha el plan de continuidad, para asegurar la continuidad de la operación o el plan de recuperación en caso de desastres para enfrentar el incidente. Por lo menos, deberá existir uno de estos planes en el Sujeto Obligado (nivel básico).

En caso de que el incidente se refiera a actos deliberados (alteración, pérdida o robo de datos personales), se deberá seguir el procedimiento que el Sujeto Obligado tenga establecido o definido (nivel básico).

En todo caso, dicho procedimiento deberá incluir las siguientes actividades, sin necesidad de que se realicen en el orden en que aparecen:

I. El responsable del personal de vigilancia deberá emitir un informe al responsable de los SDPS, en un plazo no mayor a 3 días naturales de haber ocurrido el incidente (nivel básico);

II. En caso de robo o extravío de datos personales en soportes electrónicos, el titular del Sujeto Obligado y/o el responsable de los SDPS, al tener conocimiento del incidente, deberá dar vista al órgano interno de control, al área jurídica y/o al servidor público que cuente con las facultades para presentar denuncias o querellas de cada Sujeto Obligado, en términos de sus reglamentos interiores o estatutos orgánicos, según corresponda, para que cada uno, en el ámbito de sus atribuciones, determine lo conducente (nivel básico);

III. En un plazo no mayor a 3 días naturales de haber ocurrido el incidente, el responsable de los SDPS dará aviso al público, mediante un desplegado de prensa que difunda el hecho por diversos medios, según la gravedad del caso, a escala local, regional o nacional (nivel medio), y

IV. En caso de robo o extravío de datos personales, se alertará 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 SDPS dará aviso por escrito a dichos titulares, a más tardar 5 días naturales tras haber ocurrido el incidente, recabando el acuse de recibo de esta notificación. Con anticipación a dicho escrito, si se cuenta con los datos actualizados, se deberá dar aviso por correo electrónico o por teléfono (nivel básico).

De la supervisión

Artículo 81. El Comité de Información del Sujeto Obligado deberá proponer la realización de una supervisión o verificación interna a las Unidades Administrativas que mantienen y operan SDPS, así como a los terceros contratados (nivel básico).

Capítulo Octavo
De la documentación de medidas de seguridad en procesos y políticas de los sistemas de datos personales

Capítulo Único
De la documentación de medidas de seguridad en procesos y políticas de los sistemas de datos personales

Del manual de operaciones

Artículo 82. El Sujeto Obligado deberá contar con un manual de operaciones, en el cual estén documentados los procesos y procedimientos que los servidores públicos llevan a cabo dentro del Sujeto Obligado; particularmente, 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 y responsables) interactúan con los SDPS e incorporan la adopción de las MS previstas en la Ley, en estos Lineamientos y demás disposiciones aplicables para la protección de datos personales (nivel básico).

De la sensibilización y capacitación

Artículo 83. El Sujeto Obligado deberá desarrollar cursos o pláticas de sensibilización sobre protección de datos personales en soportes físicos y en soportes electrónicos. El personal a quien deberán dirigirse estos cursos o pláticas será los servidores públicos que tengan funciones asignadas para interactuar con SDPS dentro del Sujeto Obligado (nivel básico).

Estos cursos o pláticas deberán impartirse, al menos, una vez cada año, lo cual generará el registro de asistencia correspondiente (nivel básico).

Al finalizar estos cursos o pláticas, los participantes deberán manifestar que conocen la relevancia de la protección y la seguridad de datos personales y sus responsabilidades, mediante firma autógrafa recabada en una lista que archivará el responsable de los SDPS del Sujeto Obligado (nivel básico).

Deberán existir un curso de sensibilización y un documento de firmas semejantes a los anteriores, que persigan el mismo fin, pero que estén orientados a proveedores externos que interactúan con uno o más SDPS y que deben asegurar la protección de datos personales (nivel básico).

De las cartas compromiso, cláusulas y contratos de confidencialidad

Artículo 84. Cuando menos cada dos años, el responsable de los SDPS deberá recibir y archivar una carta compromiso de parte de cada uno de los integrantes del personal autorizado que interactúa con uno o más SDPS (nivel medio).

En tal carta, el servidor público deberá manifestar, con su firma autógrafa, su compromiso para realizar su trabajo, apegándose a las MS que apliquen a los SDPS existentes en el Sujeto Obligado. Además, el servidor público deberá manifestar que conoce la Ley, estos Lineamientos y demás disposiciones aplicables que integran el marco jurídico respectivo, a fin de garantizar al titular la custodia de sus datos personales, en términos de la Ley (nivel medio).

El Sujeto Obligado deberá contar con un contrato de confidencialidad que deberá ser firmado con cada proveedor o prestador de servicios para la realización de servicios que impliquen interactuar con uno o más SDPS (nivel básico).

TÍTULO TERCERO
De la verificación de los sistemas de datos personales por el Instituto

Capítulo Primero
De la verificación y procedimiento

De la facultad de verificación

Artículo 85. El Instituto dispondrá de los medios de investigación y de la facultad de intervenir frente a la creación, modificación y supresión de SDPS sujetos al ámbito de aplicación de la Ley que no se ajusten a las disposiciones de ésta, de estos Lineamientos y de las demás disposiciones que resulten aplicables.

Para tal efecto, el Instituto tendrá acceso a los SDPS, podrá inspeccionarlos y recabar toda la información necesaria para el cumplimiento de su función de control; asimismo, podrá solicitar la exhibición o el envío de documentos y datos, así como examinarlos en el lugar en el que se encuentren instalados.

Del procedimiento de verificación

Artículo 86. El Instituto, en términos del artículo 66, fracción XIV, de la Ley, llevará a cabo visitas de verificación de la seguridad implementada en los SDPS, de conformidad con lo siguiente:

I. Toda visita de verificación deberá ajustarse a los procedimientos y las formalidades establecidos en estos Lineamientos;

II. El Instituto notificará al Sujeto Obligado el día y la hora para la práctica de la diligencia de verificación;

III. Los responsables o encargados de los SDPS objeto de verificación estarán obligados a permitir el acceso y dar facilidades e informes para el desarrollo de su labor;

IV. Al iniciar la visita, el servidor público del Instituto deberá exhibir credencial vigente con fotografía expedida por el Instituto;

V. De toda visita de verificación se levantará acta circunstanciada, en presencia de dos testigos propuestos por el responsable o el servidor público con quien se entienda la diligencia o, en su caso, por quien la practique, si aquél se hubiera negado a proponerlos;

VI. De toda acta se dejará copia al servidor público con quien se entendió la diligencia, aunque se hubiera negado a firmar, lo que no afectará la validez de la diligencia ni del documento de que se trate, siempre que el servidor público del Instituto haga constar tal circunstancia en el acta;

VII. En las actas, se hará constar:

a) Nombre del Sujeto Obligado visitado,
b) Hora, día, mes y año en que inicie y concluya la diligencia,
c) Calle, número, población o colonia, teléfono u otra forma de comunicación disponible, municipio y código postal en que se encuentre ubicado el lugar en que se practique la visita,
d) Nombre y cargo de la persona con quien se entendió la diligencia,
e) Nombre y cargo de las personas que fungieron como testigos,
f) Datos relativos a la actuación,
g) Declaración del visitado, si quiere hacerla, y
h) Nombre y firma de quienes intervinieron en la diligencia, incluyendo los de quienes la hayan llevado a cabo. Si se negara a firmar el visitado, ello no afectará la validez del acta, debiendo asentarse la razón respectiva;

VIII. La visita deberá entenderse con el responsable de los SDPS. En caso de que no se encuentre presente, la diligencia se entenderá con el encargado y, en su defecto, con quien se encuentre presente, circunstancia que se hará constar en el acta;

IX. Los visitados a quienes se haya levantado acta de verificación podrán formular observaciones en el acto de la diligencia y ofrecer pruebas relacionadas con los hechos contenidos en ella, o bien, podrán hacerlo por escrito; así como hacer uso de tal derecho dentro del término de los 5 días hábiles siguientes a la fecha en que se haya realizado la diligencia, y

X. Una vez transcurrido el plazo señalado en el numeral anterior, el área responsable del Instituto deberá emitir, dentro del término de 15 hábiles, una resolución, en la que podrá:

a) Determinar que el SDP se ajusta a lo establecido en la Ley,
b) Determinar que existen irregularidades que contravienen lo establecido en la Ley y demás normatividad aplicable, en cuyo caso formulará recomendaciones al Sujeto Obligado, a fin de que subsane las inconsistencias detectadas dentro del plazo y condiciones que al efecto se determinen,
c) El Sujeto Obligado deberá informar por escrito al Instituto, dentro del término de 5 días hábiles siguientes a que termine el plazo al que se refiere el numeral anterior, sobre la atención a las recomendaciones formuladas por el Instituto, y
d) En caso de que el Sujeto Obligado sea omiso en presentar los informes o en solventar las recomendaciones, el Instituto, en términos del artículo 66, fracción XVI, de la Ley, lo hará del conocimiento del órgano interno de control del Sujeto Obligado, para los efectos legales correspondientes, sin que tal situación lo exima del cumplimiento de los informes y recomendaciones.

En caso de que, durante la visita de verificación, se advierta un posible tratamiento ilícito de los datos personales, se estará a lo dispuesto en el artículo 71 de la Ley.

Capítulo Segundo
De la denuncia por violación a las disposiciones de la Ley

De la denuncia del titular de los datos personales
Artículo 87. En términos del artículo 32 de la Ley, el titular de los datos personales podrá presentar denuncias ante el Instituto, por posibles violaciones a las disposiciones establecidas en la misma Ley.

Al presentarse una denuncia, el Instituto deberá instaurar y desarrollar el procedimiento de verificación que se establece en estos Lineamientos, así como emitir la resolución que en derecho proceda.

TRANSITORIOS

PRIMERO. Los presentes Lineamientos entrarán en vigor al día siguiente de su publicación en el Periódico Oficial del Gobierno del Estado de México "Gaceta del Gobierno", para su debida observancia.

SEGUNDO. Los presentes Lineamientos deberán ser comunicados por el Comisionado Presidente del Instituto a los titulares de los Sujetos Obligados.

TERCERO. Se instruye al Secretario Técnico del Pleno del Instituto para que, en el ámbito de sus atribuciones conferidas, lleve a cabo las acciones conducentes para dar cumplimiento al enunciado jurídico contenido en el artículo 15.12 del Código Administrativo del Estado de México, y se publiquen los presentes Lineamientos en el Periódico Oficial del Gobierno del Estado de México "Gaceta del Gobierno" y en el sitio de internet del Instituto, así como que se comuniquen a los responsables de las Unidades de Información de los Sujetos Obligados.

ASÍ LO APROBÓ POR UNANIMIDAD EL PLENO DEL INSTITUTO DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN PÚBLICA Y PROTECCIÓN DE DATOS PERSONALES DEL ESTADO DE MÉXICO Y MUNICIPIOS, EN LA 9ª SESIÓN ORDINARIA DEL 12 DE MARZO DE 2013, Y ASÍ EL PLENO ORDENÓ LA PUBLICACIÓN DE LOS LINEAMIENTOS EN LA MISMA SESIÓN.

EL PLENO DEL INSTITUTO DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN PÚBLICA Y PROTECCIÓN DE DATOS PERSONALES DEL ESTADO DE MÉXICO Y MUNICIPIOS

ROSENDOEVGUENI MONTERREY CHEPOV
COMISIONADO PRESIDENTE
(RUBRICA).

MIROSLAVA CARRILLO MARTÍNEZ
COMISIONADA
(RUBRICA).

FEDERICO GUZMÁN TAMAYO
COMISIONADO
(RUBRICA).

IOVJAYI GARRIDO CANABAL
SECRETARIO TÉCNICO DEL PLENO
(RUBRICA).