INSTITUTO FEDERAL DE ACCESO A LA INFORMACIÓN PÚBLICA

El Pleno del Instituto Federal de Acceso a la Información Pública, con fundamento en lo dispuesto por los artículos 37 fracción IX de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, 2 fracción V de su Reglamento, y el Trigésimo Octavo y Quinto Transitorio de los Lineamientos de protección de datos personales, y:

C O N S I D E R A N D O :

Que es atribución del Instituto Federal de Acceso a la Información Pública establecer las recomendaciones sobre las políticas generales para el manejo, mantenimiento, seguridad y protección de datos personales, que estén en posesión de las dependencias y entidades de la Administración Pública Federal;

Que es necesario promover la adopción de las medidas de índole técnica y organizativa necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, con base en estándares de seguridad internacionales;

Que para lograr lo anterior, es necesario tomar en cuenta los avances tecnológicos, la naturaleza de los datos almacenados y los riesgos a que estén expuestos, ya sea que provengan de la acción humana o de las condiciones físicas y ambientales, por lo que se han establecido distintos niveles de seguridad aplicables a cada categoría o tipo de datos, alojados en los sistemas de datos personales;

Que los alcances de estas recomendaciones son los de convertirse en propuestas y sugerencias específicas para lograr la mayor protección de los datos personales, por lo que las dependencias y entidades podrán utilizarlas como modelo a seguir, para lograr con ello un estándar de seguridad, sin perjuicio de que éstas establezcan medidas adicionales que coadyuven a la mejor protección mencionada, ha tenido a bien expedir las siguientes:

RECOMENDACIONES SOBRE MEDIDAS DE SEGURIDAD APLICABLES A LOS SISTEMAS DE DATOS PERSONALES

Contenido

I. Instructivo

El presente documento es un instrumento técnico de apoyo en materia de medidas de seguridad aplicables a los sistemas de datos personales tanto físicos como automatizados, en posesión de las dependencias y entidades de la Administración Pública Federal.

Las medidas de seguridad se redactan a manera de atributos, lo cual permite utilizar cada sección como una lista de verificación, a fin de 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 facilidad si cuentan o no con la infraestructura, los procesos y los procedimientos para cumplir con las medidas de seguridad recomendadas por este documento.

Asimismo, el formato que sigue la presentación de las medidas de seguridad, permite que el responsable pueda utilizar solamente los apartados de Recomendaciones 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 podrán utilizar solamente el apartado que hace referencia a este tipo de soportes y dentro de ese apartado, únicamente las medidas correspondientes al nivel de protección que corresponda, por consiguiente, podrán omitir la revisión de otros apartados que no resulten aplicables.

II. Niveles de Seguridad

Tomando en cuenta los criterios internacionales establecidos en los reglamentos sobre medidas de seguridad para el resguardo eficaz de los datos personales, al final de cada medida sugerida se establecen niveles de seguridad, las cuales deberán observarse atendiendo a la naturaleza de la información contenida en los sistemas de datos personales.

Los niveles de seguridad responden a la mayor o menor necesidad de garantizar la integridad de los datos personales. Por lo tanto, las dependencias y entidades aplicarán el nivel básico, medio o alto de medidas de seguridad, de acuerdo con las categorías o tipos de datos personales que se detallan a continuación:

A. Nivel básico

Las medidas de seguridad marcadas con el nivel básico serán aplicables a todos los sistemas de datos personales.

A los sistemas de datos personales que contienen alguno de los datos que se enlistan a continuación, les resultan aplicables únicamente, las medidas de seguridad de **nivel básico:**

- **De Identificación:** Nombre, domicilio, teléfono particular, teléfono celular, correo electrónico, estado civil, firma, firma electrónica, RFC, CURP, cartilla militar, lugar de nacimiento, fecha de

nacimiento, nacionalidad, edad, nombres de familiares dependientes y beneficiarios, fotografía, costumbres, idioma o lengua, entre otros.

- **Laborales: D**ocumentos de reclutamiento y selección, de nombramiento, de incidencia, de capacitación, puesto, domicilio de trabajo, correo electrónico institucional, teléfono institucional, actividades extracurriculares, referencias laborales, referencias personales, entre otros.

B. Nivel medio

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

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

C. Nivel alto

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

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

III. Abreviaturas

MS. Medidas de seguridad.
SDP. Sistema de datos personales.
SDPs. Sistemas de datos personales.

IV. Definiciones

Para efectos de la aplicación de las presentes Recomendaciones, además de las definiciones contenidas en el Artículo 3 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental publicada en el Diario Oficial de la Federación el 11 de junio de 2002, en el Artículo 2 de su Reglamento, publicado en el mismo Diario el 11 de junio de 2003, y en el Lineamiento Tercero de los Lineamientos de Protección de Datos Personales expedidos por el Instituto y publicados en el Diario Oficial de la Federación el 30 de septiembre de 2005, se entenderá por:

I. Área de consulta de datos personales: El espacio destinado para que el personal autorizado examine aquellos datos personales que están autorizados a consultar, sin posibilidad de modificar su contenido.

II. Área de recepción de datos personales: El 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: El espacio para almacenar datos personales que han recibido el tratamiento correspondiente para que formen parte integral de uno o más SDPs, sin importar el soporte (físico, electrónico, o ambos) utilizado para su almacenamiento.

IV. Divulgación de incidentes: Las acciones que adoptan el Titular de la dependencia o entidad 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, etc.), los acontecimientos de caso fortuito o de fuerza mayor (desastres naturales, incendios, huelgas, etc.), 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 datos personales que forman parte de esos 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", y los que se creen posteriormente con el mismo propósito.

VII. Manual de operaciones: Conjunto de documentos que enumeran, definen y detallan los procesos y procedimientos que los servidores públicos llevan a cabo dentro de una dependencia o entidad.

VIII. Personal o Personal autorizado: Los usuarios o encargados (servidores públicos) que han recibido autorización para interactuar con uno o más SDPs por parte del Responsable de dichos sistemas.

IX. Personal de sistemas: El 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, vídeo y datos, fichas de microfilm, discos ópticos (CDs y DVDs),

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 una dependencia o entidad. Sus propósitos son precisar e informar el grado de cumplimiento entre la información recabada y los criterios establecidos.

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

Recomendaciones

1. MS para datos personales en soportes físicos

1.1. Área de recepción de datos personales

1. Existe la infraestructura apropiada —y se siguen los procesos y procedimientos necesarios y suficientes— de tal manera que es 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]
2. El personal autorizado que labora en el área de recepción ostenta una identificación con fotografía (credencial o gafete) emitida por la dependencia o entidad. [Nivel básico]
3. Cualquier persona puede identificar con facilidad al personal autorizado que labora en el área de recepción gracias a que los nombres completos y fotografías de dicho personal se exhiben en un lugar visible dentro y fuera de dicha área. [Nivel medio]
4. El Encargado de los SDPs actualiza los nombres completos y fotografías que se exhiben en el área de recepción conforme se van presentando cambios de personal. [Nivel medio]
5. No está permitido el libre acceso y el uso de aquellos aparatos referidos en la sección "4.5. Equipo no autorizado" dentro del área de recepción. [Nivel medio]
6. Existe señalización visible sobre las restricciones de acceso, las prohibiciones que aplican y el procedimiento para dar aviso al personal de vigilancia en caso de sospecharse la presencia de personas no autorizadas en el área de recepción. [Nivel básico]

1.2. Área de resguardo de datos personales

1. Existe la infraestructura apropiada —y se siguen los procesos y procedimientos necesarios y suficientes— de tal manera que es posible mantener en forma organizada y segura los datos personales en soportes físicos dentro del área de resguardo. [Nivel básico]
2. De existir ventanas o muros divisorios transparentes en el área de resguardo, la visión está obstruida mediante una película translúcida (papel albanene, por ejemplo). [Nivel medio]
3. Al interior del área de resguardo, existen las condiciones ambientales idóneas para preservar en buen estado los datos personales en soportes físicos durante el tiempo de conservación. [Nivel básico]
4. La puerta de acceso del área de resguardo cuenta con cerradura, dispositivo electrónico o cualquier otra tecnología que impida su libre apertura. Este mecanismo queda cerrado en horas no hábiles o cuando el personal autorizado que ahí labora abandona el área. [Nivel básico]
5. El mobiliario utilizado dentro del área de resguardo protege los datos personales en soportes físicos de condiciones adversas en humedad, temperatura, iluminación solar, polvo, consumo de alimentos y presencia de plagas, entre otras. [Nivel básico]
6. El mobiliario utilizado para almacenar los datos personales en soportes físicos cuenta con cerraduras, dispositivos electrónicos o cualquier otra tecnología que impida la libre apertura de sus puertas, cajones o compartimientos. Tales mecanismos quedan cerrados en horas no hábiles. [Nivel medio]

7. El personal autorizado que labora en el área de resguardo ostenta una identificación con fotografía (credencial o gafete) emitida por la dependencia o entidad. [Nivel básico]
8. Cualquier persona puede identificar con facilidad al personal autorizado que labora en el área de resguardo gracias a que los nombres completos y fotografías de dicho personal se exhiben en un lugar visible dentro y fuera de dicha área. [Nivel medio]
9. El Encargado de los SDPs actualiza los nombres completos y fotografías que se exhiben en el área de resguardo conforme se presentan cambios de personal. [Nivel medio]
10. No está permitido el libre acceso y el uso de aquellos aparatos referidos en la sección "4.5. Equipo no autorizado" dentro del área de resguardo. [Nivel medio]
11. Existe señalización visible sobre las restricciones de acceso, las prohibiciones que aplican y el procedimiento para dar aviso al personal de vigilancia en caso de sospecharse la presencia de personas no autorizadas en el área de resguardo. [Nivel básico]

1.3. Área de consulta de datos personales

1. Existe la infraestructura apropiada —y se siguen los procesos y procedimientos necesarios y suficientes— de tal manera que es posible supervisar y vigilar los datos personales en soportes físicos que consultan los Usuarios de los datos dentro del área de consulta. [Nivel básico]
2. De existir ventanas o muros divisorios transparentes en el área de consulta, la visión está obstruida mediante una película translúcida (papel albanene, por ejemplo). [Nivel medio]
3. La puerta de acceso del área de consulta cuenta con cerradura, dispositivo electrónico o cualquier otra tecnología que impida su libre apertura. Este mecanismo queda cerrado en horas no hábiles o cuando el personal autorizado que ahí labora abandona el área. [Nivel medio]
4. El personal autorizado que labora en el área de consulta ostenta una identificación con fotografía (credencial o gafete) emitida por la dependencia o entidad. [Nivel básico]
5. Cualquier persona puede identificar con facilidad al personal autorizado que labora en el área de consulta gracias a que los nombres completos y fotografías de dicho personal se exhiben en un lugar visible dentro y fuera de dicha área. [Nivel medio]
6. El Encargado de los SDPs actualiza los nombres completos y fotografías que se exhiben en el área de consulta conforme se presentan cambios de personal. [Nivel medio]
7. No está permitido el libre acceso y el uso de aquellos aparatos referidos en la sección "4.5. Equipo no autorizado" dentro del área de consulta. [Nivel medio]
8. Existe señalización visible sobre: horarios de atención, restricciones de acceso, prohibiciones que aplican y el procedimiento para dar aviso al personal de vigilancia en caso de sospecharse la presencia de personas no autorizadas en el área de consulta. [Nivel básico]

1.4. Acceso y consulta de datos personales

1.4.1. Acceso

1. Existen puntos de revisión en la dependencia o entidad en donde el personal de vigilancia controla el acceso y verifica la identidad de quienes tienen el propósito de ingresar a una zona de acceso restringido. [Nivel básico]
2. El personal que tienen intención de ingresar a una zona de acceso restringido se registra y entrega una identificación oficial con fotografía (credencial de elector, pasaporte, etc.) al personal de vigilancia que atiende dicho punto de revisión. [Nivel medio]

3. El Encargado de los SDPs es el único que autoriza la entrada al área de recepción y al área de resguardo al personal debidamente registrado, anotando el hecho como se explica en la sección "1.5. Registro de actividades". [Nivel básico]
4. En todo caso, la dependencia o entidad adopta las medidas de seguridad necesarias para el ingreso a una zona de acceso restringido.

1.4.2. Consulta

1. El usuario consulta los datos personales en soportes físicos dentro del área de consulta. [Nivel alto]
2. El Encargado de los SDPs al autorizar la salida de datos personales en soportes electrónicos o en soportes físicos, anota el hecho como se explica en la sección "1.5. Registro de actividades". [Nivel básico]

1.4.3. Personas autorizadas y no autorizadas

1. El ingreso a las zonas de acceso restringido donde existen datos personales en soportes físicos es sólo con la autorización del Encargado de los SDPs. [Nivel básico]
2. Cada acceso y consulta realizada por personas no autorizadas es considerada como un incidente de intrusión que se denuncia ante las autoridades competentes para su investigación. [Nivel medio]

1.4.4. Medidas para la prevención de intrusiones

1. El personal autorizado que labora en las zonas de acceso restringido de los SDPs verifica durante el desempeño de sus funciones que en dichas áreas no hay personas no autorizadas. [Nivel básico]
2. Además, el personal de vigilancia realiza funciones de forma permanente en las zonas de acceso restringido de los SDPs. [Nivel medio]
3. Las zonas de acceso restringido cuentan con un sistema de vídeo-vigilancia remota que permite vigilar la puerta de acceso y el interior de dichas áreas. Dicho sistema cuenta con cámaras para visión nocturna, un sistema de grabación que opere las 24 horas, los 7 días de la semana (24x7) y un archivo que acumula grabaciones de los dos meses anteriores. [Nivel alto]
4. En caso de ocurrir un incidente de intrusión, el personal de vigilancia acude de inmediato a la zona de acceso restringido presuntamente violada para corroborar el hecho. De comprobarse este, la grabación realizada por el sistema de vídeo-vigilancia remota se transfiere a un soporte físico para que pueda ser utilizado como prueba por las autoridades que investiguen el caso. [Nivel alto]

1.5. Registro de actividades

1.5.1. Operación cotidiana

1. El Responsable de los SDPs mantiene estricto control y registro de:

    a) 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]

b) La asignación, actualización y reemplazo de llaves, tarjetas, contraseñas de acceso y demás elementos que entregue a los usuarios para que éstos puedan abrir los mecanismos de apertura de puertas y mobiliario en las zonas de acceso restringido. [Nivel básico]
c) Las autorizaciones emitidas a los usuarios y demás personal debidamente registrado que solicitan acceso a las áreas de recepción o resguardo. Para ello, el Encargado anota

- Quién solicita el acceso
- Cuándo lo solicita
- Cuándo se lleva a cabo
- La razón que lo motiva [Nivel básico]

d) Las autorizaciones emitidas a los usuarios que solicitan permiso para extraer datos personales en soportes físicos del área de consulta. Para ello, el Encargado anota

- Quién hace la solicitud
- Qué documentos se lleva
- Cuándo se los lleva
- Cuándo promete devolverlos (si aplica)
- Cuándo efectivamente los devuelve (si aplica)
- Por qué necesita llevárselos [Nivel medio]

e) Las autorizaciones emitidas a los usuarios que solicitan permiso para introducir a las zonas de acceso restringido aparatos tales como los mencionados en la sección "4.5. Equipo no autorizado". Para ello, el Encargado anota

- Quién hace la solicitud
- Qué equipo introducirá
- Cuándo y por cuánto tiempo
- Por qué necesita introducirlo [Nivel medio]

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

1.5.2. Divulgación de incidentes

1. En caso de presentarse un incidente, se sigue el procedimiento que la dependencia o entidad tenga definido. [Nivel básico]

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

2. El responsable del personal de vigilancia emite un informe al Responsable de los SDPs a no más de 3 días naturales de haber ocurrido el incidente. [Nivel básico]
3. En caso de robo o extravío de datos personales en soportes físicos, el titular de la dependencia o entidad o el Responsable de los SDPs, al tener conocimiento del incidente, da vista al Órgano Interno de Control, al área jurídica y/o al servidor público que tenga facultades para presentar denuncias o querellas de cada dependencia o entidad, en términos de sus Reglamentos Interiores o Estatutos Orgánicas, según corresponda, para que cada uno, en el ámbito de sus atribuciones, determine lo conducente. [Nivel básico]

4. A no más de 3 días naturales de haber ocurrido el incidente, el Responsable de los SDPs da aviso al público mediante un desplegado de prensa que difunde el hecho por diversos medios, según la gravedad del caso, a escala local, regional o nacional. [Nivel medio]
5. En caso de robo o extravío de datos personales, se alerta a los titulares de los datos afectados para que tomen sus precauciones ante el posible uso ilegal de su información. Para tal efecto, el Responsable de los SDPs da aviso por escrito a dichos titulares, a más tardar cinco días naturales de haber ocurrido el incidente, recabando el acuse de recibo de esta notificación. Con anticipación a dicho escrito, si se cuentan con los datos actualizados, se da aviso por correo electrónico o por teléfono. [Nivel básico]

1.5.3. Supervisión

1. El Comité de información de la dependencia o entidad propone la realización de una supervisión interna para las unidades administrativas que mantienen y operan SDPs. [Nivel básico]

1.6. Baja de datos personales

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

1. El Encargado de los SDPs:
    a) Sigue procedimientos y utiliza mecanismos para asegurar la valoración y en su caso, destrucción de soportes físicos que contienen datos personales. [Nivel medio]
    b) Destruye por completo dichos soportes físicos antes de desecharlos [Nivel básico]
    c) Lleva una bitácora de las veces que se efectúa la acción de baja de datos personales. [Nivel básico]
2. Los métodos de destrucción de datos personales en soportes físicos están definidos en el Manual de operaciones de la dependencia o entidad; o, si no lo están, son aprobados por el Responsable de los SDPs antes de ejecutarlos. [Nivel básico]
3. Si en esa dependencia o entidad realizan la separación de materiales para su reciclaje (como podría suceder con el papel, el cartón, el metal y el plástico), los datos personales contenidos en materiales reciclables son triturados y la viruta resultante se entrega directamente a una empresa que los recibe para procesarlos de inmediato, garantizando por escrito que no serán examinados para su eventual reconstrucción. [Nivel medio]

2. MS para datos personales en soportes electrónicos

2.1. Área de recepción de datos personales

1. Existe la infraestructura apropiada —y se siguen los procesos y procedimientos necesarios y suficientes— de tal manera que es posible mantener en forma organizada y segura los datos personales recibidos en el área de recepción, en tanto siguen la demás fases de su tratamiento. [Nivel básico]
2. El equipo de cómputo instalado en el área de recepción cumple con las Recomendaciones presentadas en la sección "4. MS para equipo de cómputo en zonas de acceso restringido". [Nivel básico]
3. Dicho equipo de cómputo está provisto de la tecnología necesaria y suficiente para verificar la identidad del personal autorizado que labora en el área de recepción. Ello implica que, mediante la verificación de claves de acceso, dicho personal accede al equipo a fin de realizar el tratamiento que corresponda a la recepción de datos personales. [Nivel medio]
4. El personal autorizado que labora en el área de recepción ostenta una identificación con fotografía (credencial o gafete) emitida por la dependencia o entidad. [Nivel básico]
5. Cualquier persona puede identificar con facilidad al personal autorizado que labora en el área de recepción gracias a que los nombres completos y fotografías de dicho personal se exhiben en un lugar visible dentro y fuera de dicha área. [Nivel medio]
6. El Encargado de los SDPs actualiza los nombres completos y fotografías que se exhiben en el área de recepción conforme se van presentando cambios de personal. [Nivel medio]
7. No está permitido el libre acceso y el uso de aquellos aparatos referidos en la sección "4.5. Equipo no autorizado" dentro del área de recepción. [Nivel medio]
8. Existe señalización visible sobre las restricciones de acceso, las prohibiciones que aplican y el procedimiento para dar aviso al personal de vigilancia en caso de sospecharse la presencia de personas no autorizadas en el área de recepción. [Nivel básico]

2.2. Área de resguardo de datos personales

1. Existe la infraestructura apropiada —y se siguen los procesos y procedimientos necesarios y suficientes— de tal manera que es posible mantener en forma organizada y segura los datos personales en soportes electrónicos dentro del área de resguardo. [Nivel básico]
2. De existir ventanas o muros divisorios transparentes en el área de resguardo, la visión está obstruida mediante una película translúcida (papel albanene, por ejemplo). [Nivel medio]
3. Al interior del área de resguardo, existen las condiciones ambientales idóneas para preservar en buen estado los datos personales en soportes electrónicos durante el tiempo de conservación. [Nivel básico]
4. La puerta de acceso del área de resguardo cuenta con cerradura, dispositivo electrónico o cualquier otra tecnología que impida su libre apertura. Este mecanismo queda cerrado en horas no hábiles o cuando el personal autorizado que ahí labora abandona el área. [Nivel básico]
5. El equipo de cómputo instalado en el área de resguardo cumple con las Recomendaciones presentadas en la sección "4. MS para equipo de cómputo en zonas de acceso restringido". [Nivel básico]

6. Dicho equipo de cómputo está provisto de la tecnología necesaria y suficiente para verificar la identidad del usuario que labora en el área de resguardo. Ello implica que, mediante la verificación de claves de acceso, dicho personal accede al equipo a fin de realizar el tratamiento que corresponda al resguardo de datos personales. [Nivel medio]
7. El mobiliario utilizado dentro del área de resguardo protege los datos personales en soportes electrónicos de condiciones adversas en humedad, temperatura, iluminación solar, polvo, consumo de alimentos y presencia de plagas, entre otras. [Nivel básico]
8. El mobiliario utilizado para almacenar los datos personales en soportes electrónicos cuenta con cerraduras, dispositivos electrónicos o cualquier otra tecnología que impida la libre apertura de sus puertas, cajones o compartimientos. Tales mecanismos quedan cerrados en horas no hábiles. [Nivel básico]
9. El personal autorizado que labora en el área de resguardo ostenta una identificación con fotografía (credencial o gafete) emitida por la dependencia o entidad. [Nivel básico]
10. Cualquier persona puede identificar con facilidad al personal autorizado que labora en el área de resguardo gracias a que los nombres completos y fotografías de dicho personal se exhiben en un lugar visible dentro y fuera de dicha área. [Nivel medio]
11. El Encargado de los SDPs actualiza los nombres completos y fotografías que se exhiben en el área de resguardo conforme se presentan cambios de personal. [Nivel medio]
12. No está permitido el libre acceso y el uso de aquellos aparatos referidos en la sección "4.5. Equipo no autorizado" dentro del área de resguardo. [Nivel básico]
13. Existe señalización visible sobre las restricciones de acceso, las prohibiciones que aplican y el procedimiento para dar aviso al personal de vigilancia en caso de sospecharse la presencia de personas no autorizadas en el área de resguardo. [Nivel básico]

2.3. Área de consulta de datos personales

1. Existe la infraestructura apropiada —y se siguen los procesos y procedimientos necesarios y suficientes— de tal manera que es posible supervisar y vigilar los datos personales en soportes electrónicos que consultan los Usuarios de los datos dentro del área de consulta. [Nivel básico]
2. De existir ventanas o muros divisorios transparentes en el área de consulta, la visión está obstruida mediante una película translúcida (papel albanene, por ejemplo). [Nivel medio]
3. La puerta de acceso del área de consulta cuenta con cerradura, dispositivo electrónico o cualquier otra tecnología que impida su libre apertura. Este mecanismo queda cerrado en horas no hábiles o cuando el personal autorizado que ahí labora abandona el área. [Nivel medio]
4. El equipo de cómputo instalado en el área de consulta cumple con las Recomendaciones presentadas en la sección "4. MS para equipo de cómputo en zonas de acceso restringido". [Nivel básico]
5. Dicho equipo de cómputo está provisto de la tecnología necesaria y suficiente para verificar la identidad del usuario que labora en el área de consulta. Ello implica que, mediante la verificación de claves de acceso, dicho personal accede al equipo a fin de realizar el tratamiento que corresponda al resguardo de datos personales. [Nivel medio]
6. El usuario que labora en el área de consulta ostenta una identificación con fotografía (credencial o gafete) emitida por la dependencia o entidad. [Nivel básico]
7. Cualquier persona puede identificar con facilidad al personal autorizado que labora en el área de consulta gracias a que los nombres completos y fotografías de dicho personal se exhiben en un lugar visible dentro y fuera de dicha área. [Nivel medio]

8. El Encargado de los SDPs actualiza los nombres completos y fotografías que se exhiben en el área de consulta conforme se presentan cambios de personal. [Nivel medio]
9. No está permitido el libre acceso y el uso de aquellos aparatos referidos en la sección "4.5. Equipo no autorizado" dentro del área de consulta. [Nivel medio]
10. Existe señalización visible sobre: horarios de atención, restricciones de acceso, prohibiciones que aplican y el procedimiento para dar aviso al personal de vigilancia en caso de sospecharse la presencia de personas no autorizadas en el área de consulta. [Nivel básico]

2.4. Acceso y consulta de datos personales

2.4.1. Acceso

1. Existen puntos de revisión en la dependencia o entidad en donde el personal de vigilancia controla el acceso y verifica la identidad de quienes tienen el propósito de ingresar a una zona de acceso restringido. [Nivel básico]
2. El personal que tienen intención de ingresar a una zona de acceso restringido se registra y entrega una identificación oficial con fotografía (credencial de elector, pasaporte, etc.) al personal de vigilancia que atiende dicho punto de revisión. [Nivel medio]
3. El Encargado de los SDPs es el único que autoriza la entrada al área de recepción y al área de resguardo al personal debidamente registrado, anotando el hecho como se explica en la sección "2.5. Registro de actividades". [Nivel básico]
4. En todo caso, la dependencia o entidad adopta las medidas de seguridad necesarias para el ingreso a una zona de acceso restringido.

2.4.2. Consulta

1. El usuario consulta los datos personales en soportes electrónicos dentro del área de consulta. [Nivel medio]
2. El Encargado de los SDPs al autorizar la salida de datos personales en soportes electrónicos o en soportes físicos, anota el hecho como se explica en la sección "2.5. Registro de actividades". [Nivel básico]

2.4.3. Personas autorizadas y no autorizadas

1. El ingreso a las zonas de acceso restringido donde existen datos personales en soportes electrónicos es sólo con la autorización del Responsable de los SDPs. [Nivel básico]
2. Cada acceso y consulta realizada por personas no autorizadas es considerada como un incidente de intrusión que se denuncia ante las autoridades competentes para su investigación. [Nivel básico]

2.4.4. Medidas para la prevención de intrusiones

1. El personal autorizado que labora en las zonas de acceso restringido de los SDPs verifica durante el desempeño de sus funciones que en dichas áreas no hay personas no autorizadas. [Nivel básico]
2. Además, el personal de vigilancia realiza funciones de forma permanente en las zonas de acceso restringido de los SDPs. [Nivel medio]

3. El equipo de cómputo instalado en las zonas de acceso restringido cumple con las Recomendaciones presentadas en la sección "4. MS para equipo de cómputo en zonas de acceso restringido". [Nivel básico]
4. Dicho equipo de cómputo está provisto de la tecnología necesaria y suficiente para verificar la identidad del usuario que labora en estas zonas y que utiliza tal equipo. Ello implica que, mediante la verificación de claves de acceso, dicho usuario accede al equipo para interactuar con el o los SDPs que tiene autorizados. [Nivel medio]
5. Las zonas de acceso restringido cuentan con un sistema de vídeo-vigilancia remota que permite vigilar la puerta de acceso y el interior de dichas áreas. Dicho sistema cuenta con cámaras para visión nocturna, un sistema de grabación que opere las 24 horas, los 7 días de la semana (24x7) y un archivo que acumula grabaciones de los dos meses anteriores. [Nivel alto]
6. En caso de ocurrir un incidente de intrusión, el personal de vigilancia acude de inmediato a la zona de acceso restringido presuntamente violada para corroborar el hecho. De comprobarse este, la grabación realizada por el sistema de vídeo-vigilancia remota se transfiere a un soporte físico para que pueda ser utilizado como prueba por las autoridades que investiguen el caso. [Nivel alto]

2.5. Registro de actividades

2.5.1. Operación cotidiana

1. El Responsable de los SDPs mantiene estricto control y registro de:

   a) 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]

   b) La asignación, actualización y reemplazo de llaves, tarjetas, contraseñas de acceso y demás elementos que entregue a los usuarios para que éstos pueda abrir los mecanismos de apertura de puertas y mobiliario en las zonas de acceso restringido. [Nivel básico]

   c) Las autorizaciones emitidas a los usuarios y demás personal debidamente registrado que solicitan acceso a las áreas de recepción o resguardo. Para ello, el Encargado anota

      - Quién solicita el acceso
      - Cuándo lo solicita
      - Cuándo se lleva a cabo
      - La razón que lo motiva [Nivel básico]

   d) Las autorizaciones emitidas a los usuarios que solicitan permiso para extraer datos personales en soportes electrónicos del área de consulta. Para ello, el Encargado anota

      - Quién hace la solicitud
      - Qué documentos se lleva y en qué tipo de soporte (físico o electrónico)
      - Cuándo se los lleva
      - Cuándo promete devolverlos (si aplica)
      - Cuándo efectivamente los devuelve (si aplica)
      - Por qué necesita llevárselos [Nivel medio]

   b) Las autorizaciones emitidas a los usuarios que solicitan permiso para introducir a las zonas de acceso restringido aparatos tales como los mencionados en la sección "4.5. Equipo no autorizado". Para ello, el Encargado anota

- Quién hace la solicitud
- Qué equipo introducirá
- Cuándo y por cuánto tiempo
- Por qué necesita introducirlo [Nivel medio]

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

2.5.2. Divulgación de incidentes

5. En caso de presentarse un incidente, se sigue el procedimiento que la dependencia o entidad tenga definido. [Nivel básico]

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

6. El responsable del personal de vigilancia emite un informe al Responsable de los SDPs a no más de 3 días naturales de haber ocurrido el incidente. [Nivel básico]
7. En caso de robo o extravío de datos personales en soportes electrónicos, el titular de la dependencia o entidad o el Responsable de los SDPs, al tener conocimiento del incidente, da vista al Órgano Interno de Control, al área jurídica y/o al servidor público que tenga facultades para presentar denuncias o querellas de cada dependencia o entidad, en términos de sus Reglamentos Interiores o Estatutos Orgánicas, según corresponda, para que cada uno, en el ámbito de sus atribuciones, determine lo conducente. [Nivel básico]
8. A no más de 3 días naturales de haber ocurrido el incidente, el Responsable de los SDPs da aviso al público mediante un desplegado de prensa que difunde el hecho por diversos medios, según la gravedad del caso, a escala local, regional o nacional. [Nivel medio]
9. En caso de robo o extravío de datos personales, se alerta a los titulares de los datos afectados para que tomen sus precauciones ante el posible uso ilegal de su información. Para tal efecto, el Responsable de los SDPs da aviso por escrito a dichos titulares, a más tardar cinco días naturales de haber ocurrido el incidente, recabando el acuse de recibo de esta notificación. Con anticipación a dicho escrito, si se cuentan con los datos actualizados, se da aviso por correo electrónico o por teléfono. [Nivel básico]

2.5.3. Supervisión

1. El Comité de información de la dependencia o entidad propone la realización de una supervisión interna para las unidades administrativas que mantienen y operan SDPs así como para los terceros contratados que interactúan con dichos SDPs. [Nivel básico]

2.6. Baja de datos personales

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

1. Todo soporte electrónico que será dado de baja (ya sea por obsolescencia, sustitución o alguna otra causa) pasa por un proceso de preparación final antes de ser desechado. Dicho proceso incluye: la transferencia del contenido que sea preciso conservar hacia otro soporte electrónico y la destrucción, inhabilitación o daño que deje inservible dicho soporte. [Nivel básico]
2. Las únicas personas autorizadas para realizar proceso de preparación final son el área de sistemas y el personal de vigilancia. [Nivel básico]
3. Los métodos de destrucción de datos personales en soportes electrónicos están definidos en el Manual de operaciones de los SDPs; o, si no lo están, son aprobados por el Responsable de los SDPs antes de ejecutarlos. [Nivel básico]
4. El Encargado de los SDPs:

    a) Vigila que se sigan los procedimientos y se utilicen los mecanismos para asegurar la destrucción de soportes electrónicos que contienen datos personales. [Nivel básico]
    b) Lleva una bitácora donde registra la baja de soportes electrónicos que contienen datos personales anotando

        - Nombre y firma de la persona que realiza esta acción
        - Fecha y hora en la que se realiza
        - El destino que se le dará al soporte electrónico desechado
        - Nombre y firma (visto bueno) del Responsable de los SDPs [Nivel básico]

3. MS para transmisión de datos personales

3.1. Transmisión de datos personales en soportes físicos

3.1.1. Transmisión mediante traslado físico

1. La transmisión de datos personales en soportes físicos al interior de la dependencia o entidad se realiza mediante la vía elegida, de común acuerdo, entre las partes: mensajero interno, asistente secretarial, visita personal, etc. [Nivel básico]
2. La transmisión al exterior se realiza mediante un servicio de mensajería externo. En este caso, se define un destinatario primario y otro secundario por si el mensajero no encuentra al primero. [Nivel medio]
3. El paquete con datos personales en soportes físicos viaja debidamente sellado, de forma tal que sea perceptible cualquier violación o apertura no autorizada del mismo. [Nivel básico]
4. La entrega del paquete se realiza sólo si el destinatario acredita su identidad. Para ello, el destinatario presenta una identificación oficial con fotografía (credencial de elector, pasaporte, etc.) y el mensajero recaba nombre, firma y un número de referencia que aparezca en tal identificación además de la fecha de entrega. [Nivel medio]
5. El mensajero no entrega el paquete si el destinatario no puede acredita su identidad. En este caso, es imperativo que el mensajero regrese dicho paquete al transmisor. [Nivel medio]
6. El Responsable de los SDPs verifica que el mensajero entregó el paquete al destinatario. Si el transmisor detecta que dicho paquete fue entregado a otra persona, da inicio al proceso de atención de un incidente. [Nivel medio]

3.2. Transmisión de datos personales en soportes electrónicos

3.2.1. Preparación previa a la transmisión

1. Los datos personales que son enviados a un destinatario autorizado para manipularlos o procesarlos son sometidos a un proceso de preparación previa a la transmisión. En este caso, el encargado que realiza dicho proceso:
   - Genera archivos electrónicos que contengan los datos personales solicitados en un formato que permita al destinatario efectuar las operaciones que requiera [Nivel básico]
   - Somete dichos archivos a un proceso de encriptación que los proteja durante su trayecto aplicando un nivel de encriptación ALTO, no menor a 1024 bits [Nivel medio]
2. Los datos personales que son enviados a un destinatario con autorización para manipularlos o procesarlos no son reintegrados al SDP de donde fueron extraídos, a menos que el destinatario haya efectuado una corrección solicitada por el titular de los datos. [Nivel básico]
3. Los datos personales que son enviados a un destinatario No autorizado para manipularlos o procesarlos son sometidos a un proceso distinto de preparación previa a la transmisión. En este caso, el encargado que realiza dicho proceso:
   - Genera archivos electrónicos que contengan los datos personales solicitados en un formato protegido, de manera que el destinatario pueda examinar su contenido pero no pueda editarlo, copiarlo ni imprimirlo [Nivel medio]

- Somete los archivos resultantes a un proceso de encriptación que proteja los archivos durante su trayecto aplicando un nivel de encriptación MEDIO, no menor a 512 bits [Nivel medio]

3.2.2. Transmisión mediante traslado físico

1. La transmisión de datos personales en soportes electrónicos al interior de la dependencia o entidad se realiza mediante la vía elegida, de común acuerdo, entre las partes: mensajero interno, asistente secretarial, visita personal, etc. [Nivel básico]
2. La transmisión al exterior se realiza mediante un servicio de mensajería externo. En este caso, se define un destinatario primario y otro secundario por si el mensajero no encuentra al primero. [Nivel medio]
3. El paquete con datos personales en soportes electrónicos viaja debidamente sellado, de forma tal que sea perceptible cualquier violación o apertura no autorizada del mismo. Dichos soportes electrónicos contienen los archivos electrónicos resultantes del proceso de preparación previa a la transmisión. [Nivel básico]
4. La entrega del paquete se realiza sólo si el destinatario acredita su identidad. Para ello, el destinatario presenta una identificación oficial con fotografía (credencial de elector, pasaporte, etc.) y el mensajero recaba nombre, firma y un número de referencia que aparezca en tal identificación además de la fecha de entrega. [Nivel medio]
5. El mensajero no entrega el paquete si el destinatario no puede acredita su identidad. En este caso, es imperativo que el mensajero regrese dicho paquete al transmisor. [Nivel medio]
6. El Encargado de los SDPs verifica que el mensajero entregó el paquete al destinatario. Si el transmisor detecta que dicho paquete fue entregado a otra persona, da inicio al proceso de atención de un incidente. [Nivel medio]

3.2.3. Transmisión mediante redes de comunicación electrónica

1. La transmisión de datos personales en archivos electrónicos, previamente preparados para su transmisión, se realiza mediante redes de comunicación electrónica. [Nivel básico]
2. El transmisor recaba por escrito acuse de recibo del destinatario, ya sea por correo electrónico o mediante oficio enviado por fax. [Nivel medio]

3.2.4. Medidas para la prevención de intrusiones desde el exterior

1. Existen dispositivos de alta seguridad instalados en caso de que la red de comunicación electrónica (que conecta los servidores que contienen los datos personales con las computadoras que se utilizan para acceder a ellos) esté conectada a Internet.

   Los dispositivos instalados incluyen sistemas de protección perimetral (cortafuegos), de detección de intrusos, filtros de contenido, de prevención de intrusiones y de análisis de protocolos. [Nivel alto]

2. Se aplican las medidas necesarias y suficientes para que los puntos de acceso inalámbrico a la red de comunicación electrónica de la dependencia o entidad sean seguros y no existan huecos que puedan ser aprovechados por intrusos. [Nivel medio]
3. Las recomendaciones presentadas en la sección "4. MS para equipo de cómputo en zonas de acceso restringido" aplican en esta sección. [Nivel medio]

4. El personal de sistemas mantiene actualizada la memoria técnica de la red de comunicación electrónica con el fin de identificar los equipos inicialmente configurados y puestos a disposición del personal autorizado para interactuar los SDPs. [Nivel medio]
5. Si un equipo de cómputo queda en manos de una persona no autorizada o si es dado de baja, se utiliza la memoria técnica mencionada para cancelar la configuración del equipo en cuestión. [Nivel medio]
6. El personal de vigilancia o el Encargado de los SDPs, en coordinación con el área de sistemas, realiza de manera periódica y en forma programada análisis de vulnerabilidades y pruebas de intrusión controladas en la infraestructura de cómputo, almacenamiento y comunicaciones. El propósito de esta actividad es aplicar las medidas correctivas necesarias a fin de cerrar las vulnerabilidades encontradas y así evitar posibles incidentes de intrusión. [Nivel medio]

3.3. Registro de actividades

3.3.1. Operación cotidiana

1. El Encargado de los SDPs mantiene estricto control y registro de:
   a) Las autorizaciones emitidas a destinatarios que han solicitado que los datos personales en soportes electrónicos les sean transmitidos en un formato que permita manipularlos o procesarlos. [Nivel básico]
   b) Todas las transmisiones efectuadas, para ello, anota los datos necesarios para emitir informes sobre la transmisión según el lineamiento vigésimo sexto de los Lineamientos de Protección de Datos Personales publicados en el Diario Oficial de la Federación el 30 de septiembre de 2005. [Nivel básico]

3.3.2. Divulgación de incidentes

1. En caso de presentarse un incidente, se sigue el procedimiento que esa dependencia o entidad tenga definido. [Nivel básico]

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

2. El responsable del personal de vigilancia emite un informe al Responsable de los SDPs a no más de 3 días naturales de haber ocurrido el incidente. [Nivel básico]
3. En caso de robo o extravío de datos personales en soportes físicos, el titular de la dependencia o entidad o el Responsable de los SDPs, al tener conocimiento del incidente, da vista al Órgano Interno de Control, al área jurídica y/o al servidor público que tenga facultades para presentar denuncias o querellas de cada dependencia o entidad, en términos de sus Reglamentos Interiores o Estatutos Orgánicas, según corresponda, para que cada uno, en el ámbito de sus atribuciones, determine lo conducente. [Nivel básico]
4. A no más de 3 días naturales de haber ocurrido el incidente, el Responsable de los SDPs da aviso al público mediante un desplegado de prensa que difunde el hecho por diversos medios, según la gravedad del caso, a escala local, regional o nacional. [Nivel medio]
5. En caso de robo o extravío de datos personales, se alerta a los titulares de los datos afectados para que tomen sus precauciones ante el posible uso ilegal de su identidad. Para tal efecto, el

Responsable de los SDPs da aviso por escrito a dichos titulares, a más tardar cinco días naturales de haber ocurrido el incidente, recabando el acuse de recibo de esta notificación. Con anticipación a dicho escrito, si se cuentan con los datos actualizados, se da aviso por correo electrónico o por teléfono. [Nivel básico]

3.3.3. Supervisión

1. El Comité de información de la dependencia o entidad propone la realización de una supervisión a las unidades administrativas que mantienen y operan SDPs así como a los terceros contratados. [Nivel básico]

4. MS para equipo de cómputo en zonas de acceso restringido

4.1. Computadoras de escritorio

4.1.1. Recepción

1. Una computadora de escritorio asignada para uso en zonas de acceso restringido, sea nueva o usada, pasa por un *proceso de preparación inicial* a fin de instalarle solamente software autorizado, configurado para brindar mayor seguridad que la predeterminada por el fabricante. [Nivel básico]
2. El proceso de preparación inicial de la computadora de escritorio incluye, antes de instalar el software, sobrescribir con un solo valor (unos o ceros) el 100% del medio principal de almacenamiento no volátil con alguna herramienta especializada para ello. [Nivel medio]
3. La lista de software autorizado para computadoras de escritorio en sitios de acceso restringido es un documento que prepara y actualiza el área de sistemas de la dependencia o entidad. Este documento se prepara en coordinación con el Responsable de los SDPs, según las necesidades y las funciones que desempeña el personal autorizado a su cargo. [Nivel medio]
4. Las únicas personas autorizadas para realizar el proceso de preparación inicial son miembros del personal de las áreas de sistemas o de vigilancia. [Nivel medio]
5. El Encargado de los SDPs supervisa y verifica que la computadora de escritorio cumpla con los requerimientos de instalación establecidos y las configuraciones de seguridad definidas. [Nivel básico]
6. El proceso de preparación inicial de una computadora de escritorio que se asigna en zonas de acceso restringido queda registrado en un formulario. Este documento es archivado por el área de sistemas o por el personal de vigilancia. [Nivel básico]

4.1.2. Resguardo

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

4.1.3. Operación

1. Están deshabilitados (en el interior del equipo) o cancelados (en el exterior) los puertos de comunicación (USB, paralelo, serial, etc.) que no se utilizan. Los cables o dispositivos conectados a los puertos que sí se utilizan están asegurados para evitar su desconexión. Las cancelaciones pueden ser abiertas por personal autorizado del área de sistemas. [Nivel medio]
2. Están deshabilitados (en el interior del equipo) o cancelados (en el exterior) los dispositivos de almacenamiento removible (unidades de disco flexible, quemadores de CD/DVD, etc.). Las cancelaciones pueden ser abiertas por personal de sistemas. [Nivel medio]
3. No existen dispositivos de conexión inalámbrica (Wi-Fi, Bluetooth, infrarrojo, etc,) en las computadoras de escritorio asignadas dentro de las zonas de acceso restringido de los SDPs. [Nivel medio]
4. El acceso a una computadora de escritorio dentro de una zona de acceso restringido, con el propósito de realizar labores de mantenimiento preventivo y correctivo o para soporte técnico,

es exclusivo para el personal de sistemas o, para un proveedor externo subcontratado. En cualquier caso, el Responsable de los SDPs es quien autoriza, supervisa y registra el acceso archivando la autorización que emite. [Nivel básico]

4.1.4. Atención de fallas

1. Cuando se presenta una falla en una computadora de escritorio, el usuario del equipo —o, en su caso, el Responsable de los SDPs— reporta de inmediato el evento al área de sistemas y, de ser posible, toma las primeras acciones para evitar un mayor deterioro del equipo siguiendo las indicaciones que reciba del personal de sistemas. [Nivel básico]
2. En caso de que la falla requiera que la computadora de escritorio sea retirada de las zonas de acceso restringido de los SDPs para su reparación, los medios de almacenamiento no volátil son extraídos y puestos a resguardo para evitar la pérdida, robo o daño de los datos personales que contiene. Dicha operación la realiza el personal autorizado del área de sistemas. [Nivel básico]

4.1.5. Baja

1. Toda computadora de escritorio que es dada de baja (ya sea por obsolescencia, sustitución o alguna otra causa) pasa por un proceso de preparación final. [Nivel básico]
2. El proceso de preparación final incluye transferir a otro equipo los archivos que contengan información que sea preciso conservar y sobrescribir con un solo valor (unos o ceros) el 100% de los medios de almacenamiento no volátil con alguna herramienta especializada para ello. [Nivel básico]
3. Las únicas personas autorizadas para realizar el proceso de preparación final son miembros del personal de sistemas y de vigilancia. [Nivel básico]
4. El proceso de preparación final de una computadora de escritorio que se da de baja queda registrado en un formulario. Este documento es archivado por el área de sistemas o por el personal de vigilancia con el formulario que en su momento registró el proceso de preparación inicial del equipo. [Nivel básico]

4.2. Servidores

4.2.1. Recepción

19. Un servidor asignado para uso en zonas de acceso restringido, sea nuevo o usado, pasa por un proceso de preparación inicial a fin de instalarle solamente software autorizado, configurado para brindar mayor seguridad que la predeterminada por el fabricante. [Nivel básico]
20. El proceso de preparación inicial del servidor incluye, antes de instalar el software, sobrescribir con un solo valor (unos o ceros) el 100% de los medios principales de almacenamiento no volátil con alguna herramienta especializada para ello. [Nivel básico]
21. La lista de software autorizado para servidores en sitios de acceso restringido es un documento que prepara y actualiza el área de sistemas de la dependencia o entidad. Este documento se prepara en coordinación con el Responsable de los SDPs, según las necesidades y las funciones que desempeña el personal autorizado a su cargo. [Nivel básico]
22. Las únicas personas autorizadas para realizar el proceso de preparación inicial son miembros del personal de las áreas de sistemas o de vigilancia. [Nivel básico]
23. El Encargado de los SDPs supervisa y verifica que el servidor cumpla con los requerimientos de instalación establecidos y las configuraciones de seguridad definidas. [Nivel básico]

24. El proceso de preparación inicial de un servidor que se asigna en zonas de acceso restringido queda registrado en un formulario. Este documento es archivado por el área de sistemas o por el personal de vigilancia. [Nivel básico]

4.2.2. Resguardo

1. Todo servidor que está bajo la custodia del área de sistemas está instalado en un lugar que facilita adoptar:
   - Medidas de seguridad: Acceso restringido, sistema de vídeo-vigilancia remota.
   - Medidas para su buen funcionamiento: Temperatura de operación adecuada, mantenimiento preventivo y correctivo, atención inmediata en caso de fallas
   - Medidas que aseguran su operación continua: Elaboración y restauración de respaldos, sustitución rápida de partes dañadas [Nivel básico]
2. Aquel servidor que No está bajo la custodia del área de sistemas está asegurado físicamente para evitar el robo del gabinete o la sustracción de piezas o partes. Para tal propósito, está 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]

4.2.3. Operación

1. Aquel servidor que No está bajo la custodia del área de sistemas tiene deshabilitados (en el interior del equipo) o cancelados (en el exterior) los puertos de comunicación (USB, paralelo, serial, etc.) que no se utilizan. Los cables o dispositivos conectados a los puertos que sí se utilizan están asegurados para evitar su desconexión. Las cancelaciones pueden ser abiertas por personal de sistemas. [Nivel básico]
2. Aquel servidor que No está bajo la custodia del área de sistemas tiene deshabilitados (en el interior del equipo) o cancelados (en el exterior) los dispositivos de almacenamiento removible (unidades de disco flexible, quemadores de CD/DVD, etc.). Las cancelaciones pueden ser abiertas por personal de sistemas. [Nivel básico]
3. No existen dispositivos de conexión inalámbrica (Wi-Fi, Bluetooth, infrarrojo, etc,) en los servidores asignados dentro de las zonas de acceso restringido de los SDPs ni en aquellos que están bajo la custodia del área de sistemas. [Nivel básico]
4. El acceso a un servidor que No está bajo la custodia del área de sistemas, con el propósito de realizar labores de mantenimiento preventivo y correctivo o para soporte técnico, es exclusivo para el personal de sistemas o para un proveedor externo subcontratado. En cualquier caso, el Encargado de los SDPs es quien autoriza, supervisa y registra el acceso, archivando la autorización que emite. [Nivel básico]

4.2.4. Atención de fallas

1. Cuando se presenta una falla en un servidor que No está bajo la custodia del área de sistemas, el Responsable de los SDPs reporta de inmediato el evento al área de sistemas y, de ser posible, toma las primeras acciones para evitar un mayor deterioro del equipo siguiendo las indicaciones que reciba del personal de sistemas. [Nivel básico]
2. Para los servidores críticos que están bajo la custodia del área de sistemas, dicha área tiene contratada una póliza de reparación, mantenimiento preventivo y correctivo cuyo tiempo de

respuesta es suficiente para atender la criticidad de la información contenida en el equipo. [Nivel básico]

3. En caso de que la falla requiera que el servidor sea retirado de las zonas de acceso restringido de los SDPs para su reparación, los medios de almacenamiento no volátil son extraídos y puestos a resguardo para evitar la pérdida, robo o daño de los datos personales que contiene. Dicha operación la realiza el personal autorizado del área de sistemas. [Nivel básico]

4.2.5. Baja

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

4.3. Impresoras y otros equipos periféricos autorizados

4.3.1. Recepción

1. Las impresoras y los equipos periféricos autorizados (monitores, pantallas planas, etc.) usados en las zonas de acceso restringido de un SDP, sean nuevos o usados, pasan por un proceso de preparación inicial. Con ello se busca la presencia de puertos de comunicación (USB, paralelo, red local, por ejemplo) adicionales al principal que pudieran utilizarse para conectar dispositivos como los descritos en la sección "4.5. Equipo no autorizado". [Nivel medio]
2. Los puertos adicionales antes mencionados quedan inhabilitados (en el interior del equipo) o cancelados (en el exterior), mientras que los cables conectados a los puertos principales quedan asegurados para evitar su desconexión. Las cancelaciones pueden ser abiertas por el personal autorizado del área de sistemas. [Nivel medio]
3. Las únicas personas autorizadas para realizar el proceso de preparación inicial son miembros del personal de sistemas y de vigilancia. [Nivel medio]
4. El Encargado de los SDPs supervisa y verifica que el equipo de cómputo cumpla con los requerimientos de instalación establecidos y las configuraciones de seguridad definidas. [Nivel medio]
5. El proceso de preparación inicial de una impresora o de un equipo periférico autorizado que se asigna en zonas de acceso restringido queda registrado en un formulario. Este documento es archivado por el área de sistemas o por el personal de vigilancia. [Nivel medio]

4.3.2. Resguardo

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

protección, candados o cualquier otro dispositivo que impida la manipulación del equipo y el acceso físico al interior del equipo. [Nivel medio]
2. El equipo de almacenamiento removible externo se mantiene bajo custodia del área de sistemas o del personal de vigilancia. [Nivel medio]

4.3.3. Operación

1. El uso de impresoras y equipo periférico autorizado que se conecta directamente a computadoras de escritorio y servidores dentro de zonas de acceso restringido es vigilado, supervisado o, en su caso, autorizado por el Responsable de los SDPs. [Nivel medio]
2. Las únicas personas autorizadas para utilizar el equipo de almacenamiento removible externo son miembros del personal de sistemas y de vigilancia. [Nivel medio]

4.3.4. Atención de fallas

1. Cuando se presenta una falla en una impresora o en un equipo periférico autorizado, el usuario del equipo —o, en su caso, el Responsable de los SDPs— reporta de inmediato el evento al área de sistemas y, de ser posible, toma las primeras acciones para evitar un mayor deterioro del equipo siguiendo las indicaciones que reciba del personal de sistemas. [Nivel básico]
2. En caso de que la falla requiera que la impresora o el equipo periférico autorizado sea retirado de las zonas de acceso restringido de los SDPs para su reparación, de existir medios de almacenamiento no volátil, estos son extraídos y puestos a resguardo para evitar la pérdida, robo o daño de datos personales. Dicha operación la realiza el personal autorizado del área de sistemas. [Nivel básico]

4.3.5. Baja

1. Toda impresora y todo equipo periférico autorizado que son dados de baja (ya sea por obsolescencia, sustitución o alguna otra causa) pasan por un proceso de preparación final. [Nivel básico]
2. Las impresoras y los equipos periféricos autorizados que en su interior contienen uno o más medios de almacenamiento no volátil, fijos o removibles, reciben atención especial. En este caso, el proceso de preparación final incluye transferir a otro equipo los archivos que contengan información que sea preciso conservar y sobrescribir con un solo valor (unos o ceros) el 100% de los medios de almacenamiento no volátil con alguna herramienta especializada para ello. [Nivel medio]
3. Las únicas personas autorizadas para realizar el proceso de preparación final son miembros del personal de sistemas y de vigilancia. [Nivel medio]
4. El proceso de preparación final de una impresora o de un equipo periférico autorizado que se da de baja queda registrado en un formulario. Este documento es archivado por el área de sistemas o por el personal de vigilancia y se archiva con el formulario que en su momento registró el proceso de preparación inicial del equipo. [Nivel básico]

4.4. Registro de actividades e inventario

4.4.1. Control de activos (inventarios)

1. El área de sistemas lleva un inventario actualizado (independiente de aquél que lleva el área administrativa correspondiente) para todos los activos de cómputo, separados por tipo; es decir, computadoras personales, servidores, impresoras y equipos periféricos autorizados. [Nivel básico]

4.4.2. Operación cotidiana

1. El Responsable de los SDPs mantiene estricto control y registro de:

   a) Las autorizaciones emitidas al personal de sistemas o a proveedores externos subcontratados que proporcionan servicios de mantenimiento preventivo y correctivo así como soporte técnico para computadoras personales, servidores, impresoras y equipos periféricos autorizados asignados en áreas de acceso restringido. Dicho registro se lleva a cabo por el Encargado e incluye, por lo menos, los siguientes datos:

      - Causa que motiva el servicio
      - Número o identificación de activo del equipo de cómputo
      - Fecha y hora, tanto de inicio como de terminación del servicio
      - Nombre completo y firma de la o las personas que proporcionan el servicio
      - Tipo de identificación oficial que utiliza(n) dicha(s) persona(s) para acreditar su identidad (credencial de elector, pasaporte, etc.) y un número de referencia que aparezca en dicha identificación
      - Nombre y firma (visto bueno) del Responsable de los SDPs que autoriza el acceso
      - En forma opcional, se toma la fotografía de la(s) persona(s) que obtiene(n) acceso [Nivel básico]

   b) Las autorizaciones para la operación de equipo de almacenamiento removible externo por parte del personal de sistemas o de vigilancia cuando es necesario llevar a cabo respaldos de información contenida en computadoras de escritorio o servidores que No están bajo la custodia del área de sistemas. [Nivel básico]

   c) Las autorizaciones para el uso temporal de dispositivos como los que se listan en la sección "4.5. Equipo no autorizado" que se otorgan al personal autorizado que así lo solicite. Dicho registro incluye, por lo menos, los siguientes datos y documentos:

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

temporalmente en cualesquiera de las zonas de acceso restringido de los SDPs [Nivel básico]

2. El área de sistemas o el personal de vigilancia mantiene estricto control y registro de:

   a) El formulario donde se asientan los detalles del proceso de preparación inicial que se lleva a cabo para cada computadora de escritorio y cada servidor asignado en áreas de acceso restringido. Dicho registro incluye, por lo menos, los siguientes datos:

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

   b) El formulario donde se asientan los detalles del proceso de preparación inicial que se lleva a cabo para cada impresora y cada equipo periférico autorizado asignado en áreas de acceso restringido. Dicho registro incluye, por lo menos, los siguientes datos:

      - Nombre y firma de la o las personas que realizan el proceso de preparación inicial
      - Fecha y hora en la que se realiza dicho proceso, tanto la de inicio como la de finalización
      - Características del equipo (marca, modelo y número de serie) así como de los componentes de hardware al interior del equipo (marca y cantidad de la memoria volátil; marca, modelo y capacidad de los medios de almacenamiento no volátil; y demás componentes relevantes) en el momento de su recepción
      - Nombre y firma (visto bueno) dado por el Responsable de los SDPs
      - Número o identificación de activo del equipo que se asigna al equipo
      - Fecha en que el equipo queda instalado y se pone en operación
      - Área donde queda instalado el equipo [Nivel medio]

   c) El inventario actualizado de activos de cómputo, mismo que incluye, por lo menos, los siguientes datos:

      - Descripción
      - Área donde se instaló el equipo
      - Número o identificación de activo que el equipo de cómputo tenía asignado
      - Características del equipo (marca, modelo y número de serie)
      - Características de los componentes de hardware al interior del equipo (marca y modelo de la unidad de procesamiento central; marca y cantidad de la memoria volátil; marca, modelo y capacidad de los medios de almacenamiento no volátil; marca y versión del sistema operativo instalado; y demás componentes relevantes) en el momento de su recepción
      - Características de los componentes de hardware al interior del equipo (marca y modelo de la unidad de procesamiento central; marca y cantidad de la memoria volátil; marca,

modelo y capacidad de los medios de almacenamiento no volátil; marca y versión del sistema operativo instalado; y demás componentes relevantes) en el momento de su baja
- Memoria técnica de las configuraciones de red del equipo, si aplica
- Folio del formulario que registra los detalles del proceso de preparación inicial y fecha de alta en el inventario
- Folio del formulario que registra los detalles del proceso de preparación final y fecha de baja del inventario [Nivel básico]

d) El formulario donde se asientan los detalles del proceso de preparación final que se lleva a cabo para cada computadora de escritorio y cada servidor asignado en áreas de acceso restringido. Dicho registro incluye, por lo menos, los siguientes datos:

- Área donde estaba instalado el equipo
- Número o identificación de activo que el equipo de cómputo tenía asignado
- Nombre y firma de la persona que realiza el proceso de preparación final
- Fecha y hora en la que se realiza dicho proceso, tanto la de inicio como la de finalización
- Características del equipo (marca, modelo y número de serie) así como de los componentes de hardware al interior del equipo (marca y modelo de la unidad de procesamiento central; marca y cantidad de la memoria volátil; marca, modelo y capacidad de los medios de almacenamiento no volátil; marca y versión del sistema operativo instalado; y demás componentes relevantes) en el momento de su baja
- El destino que se le dará al equipo dado de baja
- Fecha en la que el equipo es efectivamente dado de baja
- Nombre y firma (visto bueno) del Responsable de los SDPs [Nivel básico]

e) El formulario donde se asientan los resultados del proceso de preparación final que se lleva a cabo para cada impresora y cada equipo periférico autorizado asignado en áreas de acceso restringido. Dicho registro incluye, por lo menos, los siguientes datos:

- Área donde estaba instalado el equipo
- Número o identificación de activo que el equipo de cómputo tenía asignado
- Nombre y firma de la persona que realiza el proceso de preparación final
- Fecha y hora en la que se realiza dicho proceso, tanto la de inicio como la de finalización
- Características del equipo (marca, modelo y número de serie) así como de los componentes de hardware al interior del equipo (marca y cantidad de la memoria volátil; marca, modelo y capacidad de los medios de almacenamiento no volátil; y demás componentes relevantes) en el momento de su recepción
- El destino que se le dará al equipo dado de baja
- Fecha en la que el equipo es efectivamente dado de baja
- Nombre y firma (visto bueno) del Responsable de los SDPs [Nivel medio]

f) El formulario en el que se registran los incidentes contiene la siguiente información:

- Registro del incidente donde se especifica: su tipo, gravedad, impacto, persona que lo detectó y personal que fue notificado.

- Los procedimientos implementados para la recuperación de los datos o aquellos procesos que permiten la pronta restauración de la operación del sistema.

- Seguimiento donde se indique el personal que interviene en la atención del incidente, la metodología aplicada, los datos recuperados, y en su caso, aquellos datos que ha sido necesario grabar manualmente en el proceso de recuperación. [Nivel básico]

4.4.3. Divulgación de incidentes

1. En caso de presentarse un incidente, se sigue el procedimiento que esa dependencia o entidad tenga definido. [Nivel básico]

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

2. El responsable del personal de vigilancia emite un informe al Responsable de los SDPs a no más de 3 días naturales de haber ocurrido el incidente. [Nivel básico]
3. En caso de robo o extravío de datos personales en soportes físicos, el titular de la dependencia o entidad o el Responsable de los SDPs, al tener conocimiento del incidente, da vista al Órgano Interno de Control , al área jurídica y/o al servidor público que tenga facultades para presentar denuncias o querellas de cada dependencia o entidad, en términos de sus Reglamentos Interiores o Estatutos Orgánicas, según corresponda, para que cada uno, en el ámbito de sus atribuciones, determine lo conducente. [Nivel básico]
4. A no más de 3 días naturales de haber ocurrido el incidente, el Responsable de los SDPs da aviso al público mediante un desplegado de prensa que difunde el hecho por diversos medios, según la gravedad del caso, a escala local, regional o nacional. [Nivel medio]
5. En caso de robo o extravío de datos personales, se alerta a los titulares de los datos afectados para que tomen sus precauciones ante el posible uso ilegal de su identidad. Para tal efecto, el Responsable de los SDPs da aviso por escrito a dichos titulares, a más tardar cinco días naturales de haber ocurrido el incidente, recabando el acuse de recibo de esta notificación. Con anticipación a dicho escrito, si se cuentan con los datos actualizados, se da aviso por correo electrónico o por teléfono. [Nivel básico]

4.4.4. Supervisión

1. El Comité de información de la dependencia o entidad propone la realización de una supervisión interna para las unidades administrativas que mantienen y operan SDPs así como a los terceros contratados. [Nivel básico]

4.5. Equipo no autorizado

4.5.1. Computadoras portátiles

1. No está permitido el libre acceso de computadoras portátiles a las zonas de acceso restringido de los SDPs. [Nivel básico]
2. Es posible autorizar el acceso temporal de computadoras portátiles siguiendo las recomendaciones descritas en el inciso "c", numeral "1", apartado "4.4.2. Operación cotidiana" de la sección "4.4. Registro de actividades e inventario". [Nivel básico]
3. En caso de que se autorice el acceso temporal de una computadora portátil, el área de sistemas o el personal de vigilancia lleva a acabo una revisión inicial del equipo. Dicha revisión incluye:

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

4. En caso de ser necesario el traslado de datos personales al equipo no autorizado, éste sería con las siguientes restricciones: sólo lectura, no para modificación, no para sustracción, no para impresión, no para quemado. [Nivel medio]
5. Al finalizar la visita, se llevará a cabo una revisión final de la computadora portátil por parte del área de sistemas o del personal de vigilancia. Dicha revisión incluye:

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

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

4.5.2. Dispositivos de almacenamiento externo

1. Sin excepción alguna, no se permite el acceso de ningún tipo de dispositivo de almacenamiento externo ajeno a la institución o sin autorización. [Nivel básico]
2. Es posible autorizar el acceso temporal de dispositivos de almacenamiento externo siguiendo las recomendaciones descritas en el inciso "c", numeral "1", apartado "4.4.2. Operación cotidiana" de la sección "4.4. Registro de actividades e inventario". [Nivel básico]
3. En caso de que se autorice el acceso temporal de dispositivos de almacenamiento externo, el área de sistemas o el personal de vigilancia lleva a acabo una revisión inicial del equipo. Dicha revisión incluye:

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

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

5. Al finalizar la visita, se llevará a cabo una revisión final de los dispositivos de almacenamiento externo por parte del área de sistemas o del personal de vigilancia. Dicha revisión incluye:
    - La revisión y el registro de la estructura de los medios de almacenamiento no volátil a fin de comprobar que el número de particiones y el espacio libre sigue siendo el mismo que en la revisión inicial, lo que permitiría detectar si hay archivos almacenados en el equipo portátil que no estaba al inicio
    - Las áreas no utilizadas (vacías) en los medios de almacenamiento no volátil se sobrescriben con un solo valor (unos o ceros) utilizando una herramienta especializada para ello [Nivel medio]
6. Por el riesgo que implica, está terminantemente prohibido el uso de dispositivos de almacenamiento externo para la transmisión de datos personales en soportes electrónicos, mediante traslado físico, sin antes haber sometido dichos datos personales a un proceso de preparación previa tal como se describe en la sección "3. MS para transmisión de datos personales". [Nivel medio]

4.5.3. Otros dispositivos no autorizados

1. Sin excepción alguna, no se permite el acceso de ningún tipo de dispositivo de almacenamiento externo portátil (memoria USB portátil, reproductor MP3, teléfono celular) ajeno a la institución. [Nivel básico]
2. Es posible autorizar el acceso temporal de estos dispositivos siguiendo las recomendaciones descritas en el inciso "c", numeral "1", apartado "4.4.2. Operación cotidiana" de la sección "4.4. Registro de actividades e inventario". [Nivel básico]
3. Por el riesgo que implica, está prohibido el uso de dispositivos no autorizados para la transmisión de datos personales en soportes electrónicos, mediante traslado físico, sin antes haber sometido dichos datos personales a un proceso de preparación previa tal como se describe en la sección "3. MS para transmisión de datos personales". [Nivel básico]
4. Está prohibido introducir objetos que pudiesen dañar o alterar los soportes físicos y electrónicos que contengan datos personales tales como: tijeras, navajas, marcadores, alimentos o líquidos, entre otros. [Nivel básico]

5. MS para asegurar continuidad y enfrentar desastres

5.1. Respaldo y recuperación de sistemas de datos personales automatizados

5.1.1. Medios de almacenamiento autorizados y no autorizados

1. Los medios de almacenamiento no volátil autorizados para la generación y almacenamiento de copias de seguridad (o respaldos) se dividen en dos grupos: fijos y removibles. Los medios fijos son los discos duros internos. Los medios removibles, pueden ser (i) magnéticos (cintas, discos duros externos), (ii) ópticos (CDs, DVDs) o (iii) magneto-ópticos (discos magneto-ópticos). [Nivel básico]
2. Los medios de almacenamiento no volátil autorizados se utilizan solos o en combinación, según las necesidades de respaldo y de restauración para garantizar la operación continua del SDP. [Nivel básico]
3. El uso de las unidades para lectura y escritura de dichos medios autorizados es exclusivo para el personal de sistemas, quien se encarga de generar las copias de seguridad. Ello implica que, si se trata de unidades internas (dentro del gabinete de la computadora), existe cuando menos una forma de restringir su uso. Por otro lado, si se trata de unidades externas que se conectan a un puerto de comunicaciones, entonces existe cuando menos una forma de restringir el uso de dicho puerto. [Nivel básico]
4. Todos aquellos medios de almacenamiento —así como sus respectivas unidades para lectura y escritura— que no entren dentro de las descripciones anteriores son considerados *no autorizados*. Esto incluye los dispositivos portátiles que cuenten con memoria no volátil integrada y algún dispositivo de comunicación (por cable o inalámbrica) que permita el intercambio de datos con una computadora. Algunos ejemplos son los llamados "memory-sticks", las agendas digitales, los teléfonos celulares inteligentes, las cámaras digitales de instantáneas fijas o vídeo y los dispositivos portátiles para reproducción de música/vídeo como el Apple iPod y similares. [Nivel básico]
5. El Encargado de los SDPs, en colaboración con el personal de seguridad, ha implementado medidas para restringir el acceso y el uso de los dispositivos no autorizados. Los puntos de revisión y los sistemas de vídeo-vigilancia remota coadyuvan a este propósito. [Nivel básico]

5.1.2. Inventario y clasificación de medios

1. Existe un inventario de los equipos autorizados para almacenar información crítica así como de aquellos que se utilizan para generar copias de seguridad (respaldos) de la información. [Nivel básico]
2. Los medios de almacenamiento no volátil que contienen las copias de seguridad mencionadas son clasificados y protegidos por el área de sistemas o el personal de vigilancia a fin de evitar su extravío, robo o daño accidental. [Nivel básico]
3. Se siguen 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 lleva un control por cada una. El propósito es reducir el tiempo de espera para localizar los archivos que sea necesario restaurar. [Nivel básico]

5.1.3. Almacenamiento de respaldos

1. El almacenamiento de los respaldos (es decir, de los medios de almacenamiento removibles que los contienen) se realiza en lugares seguros, preferentemente en bóvedas de seguridad. [Nivel medio]
2. El reemplazo de dichos medios de almacenamiento se lleva a cabo mediante un esquema calendarizado. Por ejemplo, un esquema de reemplazo mínimo incluye realizar un respaldo general cada 7 días, mismo que se almacena durante un mes, antes de reemplazarlo. En la bóveda, quedan siempre cuatro semanas de respaldo. [Nivel medio]
3. Los respaldos se llevan a cabo a diario, en modo incremental y en línea, en caso de que el sistema lo permita. El séptimo día se realiza un respaldo general, fuera de línea, el cual es llevado, como lo menciona el punto anterior, a un lugar seguro para su resguardo. [Nivel básico]
4. Se lleva registro de las veces que un respaldo se introduce en, o se extrae de, las bóvedas. Son sólo dos (y cuando mucho tres) personas las que estén autorizadas para realizar dichos tramites. [Nivel medio]

5.2. Operación continua de sistemas de datos personales automatizados

5.2.1. Sitios alternos

1. Existe un sitio alterno para restablecer la operación de un SDP automatizado, en el menor tiempo posible, en caso de un desastre. Para ello, se tiene establecido SOLAMENTE UNO de los siguientes tres tipos de sitios:

    a) **Sitio alterno *frío*.** En este tipo de sitios alternos no se incluye ningún equipo de cómputo ni otros recursos, de no ser por un ambiente mínimo de operación que incluya aire acondicionado, corriente eléctrica, enlaces de comunicaciones, piso falso, etc. Este tipo de sitios alternos es el menos costoso y a la vez el que más demora supone para restaurar las operaciones de un SDP automatizado.

    b) **Sitio alterno *tibio*.** En este tipo de sitios alternos el equipo esta disponible unas cuantas horas después de ocurrido el desastre pero el equipo no contiene datos personales ni software. Este tipo de sitios alternos es el punto medio en costo y en tiempo para restaurar las operaciones de un SDP automatizado.

    c) **Sitio alterno *caliente*.** En este tipo de sitios alternos se mantienen disponibles tanto el equipo como el software y los datos personales, en cualquier momento, y solo es necesario "dar la orden" para activarlo y hacer posible su operación en un tiempo mucho más corto que en los sitios alternos anteriores. Este tipo de sitios alternos es el más costoso pero el que menor demora supone para restaurar las operaciones de un SDP automatizado. [Nivel básico]

2. Dependiendo de la criticidad de un SDP automatizado, el Manual de operaciones tiene definido el tiempo requerido para su restauración como sigue: (i) no esencial, se restaura en 30 días naturales, (ii) normal, en 7 días naturales, (iii) importante, en 72 hrs., (iv) urgente, en 24 hrs., (v) crítica o esencial, de 1 a 4 horas. Estos tiempos dan pauta para elegir el sitio alterno a utilizar. [Nivel básico]

5.2.2. Tecnologías de información y telecomunicaciones

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

instalaciones de la dependencia o entidad, en otra ciudad, a kilómetros de distancia. [Nivel básico]

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

5.2.3. Personal para emergencias

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

5.3. Registro de actividades

5.3.1. Pruebas y simulacros

1. El Responsable de los SDPs, en coordinación con el área de sistemas y el personal de vigilancia, lleva a cabo pruebas y simulacros para minimizar riesgos en caso de presentarse alguna eventualidad adversa y para comprobar que los sistemas de seguridad y prevención funcionan correctamente y en el tiempo estimado como óptimo. Estas tareas se llevan a cabo periódicamente, según el nivel de criticidad de la información. [Nivel básico]
2. Existe un registro de pruebas y simulacros que contiene, cuando menos, los siguientes datos:

   - Fecha y hora, tanto de inicio como de finalización
   - Encargado de realizarlas
   - Encargado de evaluarlas
   - Tiempo de restauración
   - Firma (visto bueno) de los Responsables
   - Observaciones
   - Sugerencias de mejora

   El propósito de este registro es permitir su análisis y evaluación a fin de realizar las adecuaciones necesarias antes de que se presente una contingencia. [Nivel básico]

5.3.2. Divulgación de incidentes

1. En caso de que el incidente se refiera a la pérdida de información debida a fallas en el equipo o en sus dispositivos de almacenamiento, ya sea por fallas en instalaciones, acontecimientos de casos fortuitos o de fuerza mayor (desastres naturales, incendios, huelgas, etc.), entonces procede la declaración de este. En ese momento, se pone en marcha el Plan de Continuidad del Negocio, para asegurar la continuidad de la operación o el Plan de Recuperación en caso de

desastres para enfrentar el incidente. Cuando menos existe uno de estos planes en la dependencia o entidad. [Nivel básico]
2. En caso de que el incidente se refiera a actos deliberados (alteración, pérdida o robo de datos personales), se sigue el procedimiento que esa dependencia o entidad tenga definido. [Nivel básico]

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

3. El responsable del personal de vigilancia emite un informe al Responsable de los SDPs a no más de 3 días naturales de haber ocurrido el incidente. [Nivel básico]
4. En caso de robo o extravío de datos personales en soportes electrónicos, el titular de la dependencia o entidad o el Responsable de los SDPs, al tener conocimiento del incidente, da vista al Órgano Interno de Control, al área jurídica y/o al servidor público que tenga facultades para presentar denuncias o querellas de cada dependencia o entidad, en términos de sus Reglamentos Interiores o Estatutos Orgánicas, según corresponda, para que cada uno, en el ámbito de sus atribuciones, determine lo conducente. [Nivel básico]
5. A no más de 3 días naturales de haber ocurrido el incidente, el Responsable de los SDPs da aviso al público mediante un desplegado de prensa que difunde el hecho por diversos medios, según la gravedad del caso, a escala local, regional o nacional. [Nivel medio]
6. En caso de robo o extravío de datos personales, se alerta a los titulares de los datos afectados para que tomen sus precauciones ante el posible uso ilegal de su información. Para tal efecto, el Responsable de los SDPs da aviso por escrito a dichos titulares, a más tardar cinco días naturales de haber ocurrido el incidente, recabando el acuse de recibo de esta notificación. Con anticipación a dicho escrito, si se cuentan con los datos actualizados, se da aviso por correo electrónico o por teléfono. [Nivel básico]

5.3.3. Supervisión

1. El Comité de información de la dependencia o entidad propone la realización de una supervisión interna a las unidades administrativas que mantienen y operan SDPs así como a los terceros contratados. [Nivel básico]

6. Documentación de MS en procesos y políticas del SDP

6.1. Manual de operaciones

1. Existe un Manual de operaciones donde están documentados los procesos y procedimientos que los servidores públicos llevan a cabo dentro de la dependencia o entidad. Aquellos procesos y procedimientos en los que se describe la forma en que los titulares de los datos y los servidores públicos (usuarios, personal autorizado, encargados, responsables) interactúan con los SDPs, incorporan la adopción de estos MS recomendados para la protección de datos personales. [Nivel básico]

6.2. Sensibilización y capacitación

1. Se ha desarrollado un curso de sensibilización sobre protección de datos personales en soportes físicos y soportes electrónicos. El personal a quien va dirigido este curso son servidores públicos que tienen funciones asignadas para interactuar con SDP´s al interior de la dependencia o entidad. [Nivel básico]
2. Este curso se imparte al menos una vez cada año al personal, llevando un registro de asistencia. [Nivel básico]
3. Al finalizar el curso, el participante manifiesta conocer la relevancia de la seguridad de datos personales y sus responsabilidades mediante firma autógrafa que se recaba en una lista que archiva el Responsable de los SDPs en la dependencia o entidad. [Nivel básico]
4. Existen un curso de sensibilización y un documento de firmas, similares a los anteriores, que persiguen el mismo fin pero que están orientados a proveedores externos que interactúan con uno o más SDPs y a quienes también se exige aseguren la protección de datos personales. [Nivel básico]

6.3. Cartas compromiso, cláusulas y contratos de confidencialidad

1. Al menos cada dos años, el Responsable de los SDPs recibe (y archiva) una carta compromiso de parte de cada uno de los miembros del personal autorizado que interactúa con uno o más SDPs. [Nivel medio]
2. En dicha carta, el servidor público manifiesta, con su firma autógrafa, su compromiso para realizar su trabajo apegándose a los MS que apliquen a los SDPs en esa dependencia o entidad. Además, el servidor público manifiesta conocer los Lineamientos, el Reglamento y la Ley que integran el marco jurídico de las presentes Recomendaciones a fin de garantizar al ciudadano la custodia de sus datos personales. [Nivel medio]
3. La dependencia o entidad cuenta con un contrato de confidencialidad que ha firmado con cada proveedor o prestador de servicios que llama para la realización de servicios que impliquen interactuar con los SDPs. [Nivel básico]