1. Medidas de Seguridad para Datos Personales en Soportes Físicos.		
Número	Apartado	Disposición.
1.1.3.	1.1. Área de recepción de datos personales	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]
1.1.5.	1.1. Área de recepción de datos personales	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]
1.1.6.	1.1. Área de recepción de datos personales	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]
1.2.8.	1.2. Área de resguardo de datos personales	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]
1.2.10.	1.2. Área de resguardo de datos personales	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]
1.2.11.	1.2. Área de resguardo de datos personales	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]
1.3.5.	1.3. Área de consulta de datos personales	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]
1.3.7.	1.3. Área de consulta de datos personales	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]
1.3.8.	1.3. Área de consulta de datos personales	Existe señalización visible sobre: horarios de atención a visitantes, 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]
1.4.1.1.	1.4. Acceso y consulta de datos personales 1.4.1. Acceso	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 visitar una zona de acceso restringido. [Nivel básico]
1.4.1.2.	1.4. Acceso y consulta de datos personales 1.4.1. Acceso	Las personas que tienen intención de visitar una zona de acceso restringido se registran y entregan una identificación oficial con fotografía (credencial de elector, pasaporte, etc.) al personal de vigilancia que atiende dicho punto de revisión. [Nivel medio]
1.4.1.3.	1.4. Acceso y consulta de datos personales 1.4.1. Acceso	Los visitantes debidamente registrados en el punto de revisión obtienen y portan en todo momento y de manera visible un gafete que les será canjeado a su salida por la identificación oficial que entregaron. [Nivel medio]
1.4.1.4.	1.4. Acceso y consulta de datos personales 1.4.1. Acceso	El Encargado de los SDPs es el único que autoriza la entrada al área de recepción y al área de resguardo a los visitantes debidamente registrados, anotando el hecho como se explica en la sección "1.5. Registro de actividades". [Nivel básico]
1.5.1.1. inc. c)	1.5. Registro de actividades. 1.5.1. Operación cotidiana.	El Responsable de los SDPs mantiene estricto control y registro de: c) Las autorizaciones emitidas a los usuarios y visitantes debidamente registrados 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]
1.5.1.1. inc. d)	1.5. Registro de actividades. 1.5.1. Operación cotidiana.	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]
1.5.1.1. inc. e)	1.5. Registro de actividades. 1.5.1. Operación cotidiana.	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]
1.5.2.4.	1.5.2. Divulgación de incidentes	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]
1.5.2.5.	1.5.2. Divulgación de incidentes	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]
1.6.3.	1.6. Baja de datos personales	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. Medidas de Seguridad para Datos Personales en Soportes Electrónicos.		
2.1.5.	2.1. Área de recepción de datos personales	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]
2.1.7.	2.1. Área de recepción de datos personales	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]
2.1.8.	2.1. Área de recepción de datos personales	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]
2.2.10.	2.2. Área de resguardo de datos personales	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]
2.2.12.	2.2. Área de resguardo de datos personales	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]
2.2.13.	2.2. Área de resguardo de datos personales	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]
2.3.7.	2.3. Área de consulta de datos personales	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]
2.3.9.	2.3. Área de consulta de datos personales	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]
2.3.10.	2.3. Área de consulta de datos personales	Existe señalización visible sobre: horarios de atención a visitantes, 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]
2.4.1.1.	2.4. Acceso y consulta de datos personales. 2.4.1. Acceso	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 visitar una zona de acceso restringido. [Nivel básico]
2.4.1.2.	2.4. Acceso y consulta de datos personales. 2.4.1. Acceso	Las personas que tienen intención de visitar una zona de acceso restringido se registran y entregan una identificación oficial con fotografía (credencial de elector, pasaporte, etc.) al personal de vigilancia que atiende dicho punto de revisión. [Nivel medio]
2.4.1.3.	2.4. Acceso y consulta de datos personales. 2.4.1. Acceso	Los visitantes debidamente registrados en el punto de revisión obtienen y portan en todo momento y de manera visible un gafete que les será canjeado a su salida por la identificación oficial que entregaron. [Nivel medio]
2.4.1.4.	2.4. Acceso y consulta de datos personales. 2.4.1. Acceso	El Encargado de los SDPs es el único que autoriza la entrada al área de recepción y al área de resguardo a los visitantes debidamente registrados, anotando el hecho como se explica en la sección "2.5. Registro de

		actividades". [Nivel básico]
2.5.1.1. inc. c)	2.5. Registro de actividades 2.5.1. Operación cotidiana	El Responsable de los SDPs mantiene estricto control y registro de: c) Las autorizaciones emitidas a los usuarios y visitantes debidamente registrados 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]
2.5.1.1. inc. d)	2.5. Registro de actividades 2.5.1. Operación cotidiana	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]
2.5.1.1. inc. e)	2.5. Registro de actividades 2.5.1. Operación cotidiana	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]
2.5.2.4.	2.5.2. Divulgación de incidentes	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]
2.5.2.5.	2.5.2. Divulgación de incidentes	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]
2.5.3.1.	2.5.3. Supervisión	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]
3. Medidas de Seguridad para la Transmisión de Datos Personales.		
3.2.2.4.	3.2.2. Transmisión mediante traslado físico	La entrega del paquete se realiza sólo si el destinatario acredita su identidad. Para ello, el destinatario presenta una identificación oficial con fotografía (credencial de elector, pasaporte, etc.) y el mensajero recaba nombre, firma y un número de referencia que aparezca en tal identificación además de la fecha de entrega. [Nivel medio]
3.2.3.2.	3.2.3. Transmisión mediante redes de comunicación electrónica	El transmisor recaba por escrito acuse de recibo del destinatario, ya sea por correo electrónico o mediante oficio enviado por fax. [Nivel medio]
3.3.2.4.	3.3.2. Divulgación de incidentes	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]
3.3.2.5.	3.3.2. Divulgación de incidentes	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]
3.3.3.1.	3.3.3. Supervisión	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		
4.4.2.1.	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] 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 visitante 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]
4.4.3.4.	4.4.3. Divulgación de incidentes	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]

4.4.3.5.	4.4.3. Divulgación de incidentes	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]
4.4.4.1.	4.4.4. Supervisión	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]
4.5.2.1.	4.5.2. Dispositivos de almacenamiento externo	Sin excepción alguna, no se permite el acceso de ningún tipo de dispositivo de almacenamiento externo ajeno a la institución o sin autorización. En caso de que el visitante lleve alguno, dicho dispositivo tendrá que resguardarse en el punto de revisión, bajo custodia del personal de seguridad, o con el Responsable de los SDPs. [Nivel básico]
4.5.3.1.	4.5.3. Otros dispositivos no autorizados	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. En caso de que el visitante lleve alguno, dicho dispositivo tendrá que resguardarse en el punto de revisión, bajo custodia del personal de seguridad, o con el Responsable de los SDPs. [Nivel básico]
5. MS para asegurar continuidad y enfrentar desastres		
5.3.2.5.	5.3.2. Divulgación de incidentes	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]
5.3.2.6.		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]
5.3.3.1.	5.3.3. Supervisión	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		
6.1.1.	6.1. Manual de operaciones	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]
6.2.4.	6.2. Sensibilización y capacitación	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]
6.3.1.	6.3. Cartas compromiso, cláusulas y contratos de confidencialidad	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]