RESOLUCIÓN 622 DE 2016

(05 DIC 2016)

Por la cual establece la Política de Seguridad y Privacidad de la Información y se definen lineamientos frente su uso y manejo.

LA DIRECTORA GENERAL DEL INSTITUTO NACIONAL PARA SORDOS " INSOR"

En uso de sus facultades legales

en uso de sus facultades legales y estatutarias señaladas en el Decreto 2106 de 2013 las Leyes 87 de 1993, el artículo 78 de la Ley 489 de 1998 y el artículo 2.2.9.1.2.3 del Decreto número 1078 de 2015, y

CONSIDERANDO:

Que la Constitución Política de Colombia en su artículo 15, consagra que todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, debiendo el Estado respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en los bancos de datos y en archivos de entidades públicas y privadas;

Que la Constitución Política de Colombia, en su artículo 209 establece que la administración pública, en todos sus órdenes, tendrá un control interno, el cual se ejercerá en los términos que señale la ley y así mismo, en su artículo 269 impone a las autoridades de las entidades públicas la obligación de diseñar y aplicar, según la naturaleza de sus funciones, métodos y procedimientos de control interno;

Que el Instituto Nacional Para Sordos - INSOR mediante Resolución número 175 de 2016, reorganizó el Sistema Integrado de Gestión y asignó roles y responsabilidades en los ejes que lo integran.

Que el Decreto número 1078 de 2015 dispone que las entidades que conforman la administración pública serán sujetos obligados para el cumplimiento de las políticas y los lineamientos de la Estrategia de Gobierno en Línea, estableciendo en su artículo 2.2.9.1.2.1como uno de sus cuatro componentes el de la Seguridad y privacidad de la Información, comprendido por las acciones transversales a los componentes de TIC para Servicios, TIC para el Gobierno Abierto y TIC para la Gestión, tendientes a proteger la información y sistemas de información, del acceso, divulgación, interrupción o destrucción no autorizada;

Que es obligación del INSOR adoptar la Política de Seguridad y Privacidad de la Información y definir lineamientos frente su uso y manejo, teniendo en cuenta la normativa vigente de protección de datos personales, así como de transparencia y acceso a la información;

Que, de acuerdo con lo anterior,

RESUELVE:

CAPÍTULO I.

DISPOSICIONES GENERALES.

ARTÍCULO 1o. OBJETO. La presente resolución tiene como objeto la adopción de la política general de Seguridad y Privacidad de la información del Instituto Nacional para Sordos INSOR, así como definir lineamientos frente a su uso y manejo.

ARTÍCULO 2o. POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN. El INSOR protege, preserva y administra la integridad, confidencialidad y disponibilidad de la información en el marco de la operación de sus procesos y en cumplimiento de los requisitos legales y reglamentarios, mediante la prevención de incidentes de seguridad de la información a través de gestión de riesgos e implementación de mecanismos de seguridad físicos y lógicos, orientados a la mejora continua en la gestión y el alto desempeño del Sistema de Gestión de Seguridad y Privacidad de la Información, con la finalidad de prestar servicios con calidad y transparencia a la Población Sorda colombiana.

ARTÍCULO 3o. ÁMBITO DE APLICACIÓN. El contenido de esta política de Seguridad y privacidad de la Información, aplica a toda la entidad, sus funcionarios, contratistas y terceros y la ciudadanía en general, cuando en desarrollo de la misión institucional y cumplimiento de sus objetivos estratégicos, se adelanten acciones de recolección, procesamiento, almacenamiento, recuperación, intercambio y consulta de información.

ARTÍCULO 4°. OBJETIVOS.

1. Brindar mecanismos de aseguramiento para el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información del INSOR.
2. Mitigar los incidentes de o Privacidad de la Información en el Instituto.
3. Establecer los lineamientos necesarios para el manejo de la información y los recursos tecnológicos de la entidad.
4. Gestionar los riesgos de Seguridad y Privacidad de la información.
5. Mantener la confianza de los funcionarios, contratistas y terceros.
6. Implementar el sistema de gestión de Seguridad y Privacidad de la información.
7. Proteger los activos de información.
8. Fortalecer la cultura de Seguridad y Privacidad de la información en los funcionarios, terceros, aprendices, practicantes y clientes del Instituto.
9. Garantizar la continuidad del negocio frente a incidentes.

CAPÍTULO II.

POLÍTICAS GENERALES DE MANEJO DE INFORMACIÓN.

ARTÍCULO 5°. TRATAMIENTO DE LA INFORMACIÓN. Para el tratamiento de la información de los niños, niñas, adolescentes sordos y familias con integrantes sordos, a las cuales se les presta el acompañamiento en el marco del mandato legal encargado por el Gobierno nacional al INSOR, así como la información de los servidores públicos y colaboradores que participan en el desarrollo de las funciones de dicha disposición, el INSOR cuenta con la *"Política de Tratamiento de Datos Personales del Instituto Nacional para Sordos" con la cual se da* cumplimiento a lo dispuesto en la Ley 1581 de 2012, reglamentada por el Capítulo 25 del Título 2 de la Parte 2 del Libro

2 del Decreto número 1074 de 2015, la Ley 1712 de 2014, reglamentada por el Capítulo 2 del Título 1 de la Parte 1 del Decreto número 1081 de 2015, y las demás normas externas o internas que los modifiquen, adicionen o complementen.

ARTÍCULO 6°. POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LOS RECURSOS HUMANOS. El INSOR a través del Grupo de Talento Humano debe propender por que los servidores públicos de la entidad entiendan sus responsabilidades frente a la seguridad de la información, con el fin de reducir el riesgo de robo, fraude, mal uso de las instalaciones y medios, asegurando la confidencialidad, disponibilidad e integridad de la información.

PARÁGRAFO. El área de Contratación del INSOR incluirá en las minutas de los contratistas, cualquiera que sea su modalidad, las cláusulas u obligaciones correspondientes a la Seguridad y Privacidad de la información, con el fin de reducir el riesgo de robo, fraude, mal uso de las instalaciones y medios, asegurando la confidencialidad, disponibilidad e integridad de la información.

ARTÍCULO 7°. POLÍTICA DE GESTIÓN DE ACTIVOS. El INSOR a través de la Oficina Asesora de Planeación y Sistemas, establecerá y divulgará los lineamientos específicos para la identificación, clasificación y buen uso de los activos de información, con el objetivo de garantizar su protección.

a) **Inventario de Activos:** Los activos del INSOR deben ser identificados, clasificados y controlados para garantizar su uso adecuado, protección y la recuperación ante desastres. Por tal motivo, se debe llevar el inventario de los activos de información de propiedad del Instituto, discriminado por procesos y de acuerdo con la Guía de Inventario y Clasificación de Activos.

Para efectos de implantar los controles de Seguridad y Privacidad, las dependencias que tienen la custodia de la información generada en el marco de su función, se encargarán de proteger la información y de mantener y actualizar el inventario de activos de información relacionados con sus servicios (Información, software, hardware y recurso humano);

b) **Archivos de Gestión:** El Grupo de Servicios Administrativos será el responsable de implementar los controles necesarios para que los archivos de gestión cuenten con los mecanismos de Seguridad y Privacidad, con el fin de proteger y conservar la confidencialidad, integridad y disponibilidad de la información del Instituto;

c) **Clasificación de la Información:** La clasificación de la información del INSOR se realizará de conformidad con la Ley 1712 de 2014 reglamentada por el Capítulo 2 del Título 1 de la Parte 1 del Decreto número 1081 de 2015, la Ley 594 de 2000 (Ley General de Archivos), el Decreto número 1080 de 2015 y lo estipulado en la misma Guía de Inventario y Clasificación de Activos del Instituto.

ARTÍCULO 8°. RESPONSABILIDADES DE LOS SERVIDORES PÚBLICOS Y CONTRATISTAS FRENTE AL USO DE LOS RECURSOS TECNOLÓGICOS. Todos los colaboradores que hagan uso de los activos de información del INSOR, tienen la responsabilidad de cumplir las políticas establecidas para el uso adecuado de los activos de información, entendiendo que el inadecuado uso de los recursos, puede poner en riesgo el cumplimiento de la misión institucional o continuidad del negocio.

a) **Uso del correo electrónico:** El servicio de correo electrónico institucional es una herramienta de apoyo a las funciones y responsabilidades de los funcionarios y contratistas del INSOR. Para el logro del mejor uso de esta herramienta, se establecen los siguientes lineamientos:

1. El servicio de correo electrónico institucional debe ser empleado únicamente para enviar y recibir mensajes de carácter institucional. En consecuencia, no puede ser utilizado con fines personales, económicos, comerciales y/o cualquier otro ajeno a los propósitos de la Entidad.
2. En cumplimiento de la iniciativa institucional del uso aceptable del papel y la Eficiencia Administrativa, se debe preferir el uso del correo electrónico al envío de documentos físicos, siempre que la ley lo permita.
3. Los mensajes de correo están respaldados por la Ley 527 de 1999 (por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones), establece la legalidad de los mensajes de datos y las implicaciones legales que conlleva el mal uso de éstos.
4. Está prohibido el envío de correos masivos (más de 50 destinatarios) a nivel nacional tanto internos como externos, salvo a través de la Dirección General, las Subdirecciones, La Secretaría General, Área de Comunicaciones, Oficina Asesora de Planeación y Sistemas.
5. Todo mensaje SPAM o CADENA debe ser inmediatamente reportado a la Oficina Asesora de Planeación y Sistemas a través de la Mesa de Servicios – GLPI, como incidente de Seguridad de la información según procedimiento establecido. No está permitido el envío y/o reenvío de mensajes en cadena.
6. Todo mensaje sospechoso respecto de su remitente o contenido debe ser inmediatamente reportado a la Oficina Asesora de Planeación y Sistemas, a través de la Mesa de Servicios - GLPI, como incidente de seguridad de la información según procedimiento establecido y proceder de acuerdo con las indicaciones de esta área. Lo anterior, debido a que puede ser contentivo de virus, en especial si contiene archivos adjuntos con extensiones .exe, .bat, .prg, .bak, .pif, tengan explícitas referencias no relacionadas con la misión de la Entidad (como por ejemplo: contenidos eróticos, alusiones a personajes famosos).
7. La cuenta de correo institucional no debe ser revelada en páginas o sitios publicitarios, de comercio electrónico, deportivos, agencias matrimoniales, casinos, o a cualquier otra ajena a los fines del INSOR.
8. Está expresamente prohibido el uso del correo para la transferencia de contenidos insultantes, ofensivos, injuriosos, obscenos, violatorios de los derechos de autor y/o que atenten contra la integridad moral de las personas o instituciones.
9. Está expresamente prohibido distribuir información del INSOR no pública, a otras entidades o ciudadanos sin la debida autorización de la Dirección General, Subdirecciones y/o Oficina Asesora de Planeación y Sistemas.
10. El cifrado de los mensajes de correo electrónico institucional será necesario, siempre que la información transmitida esté clasificada como confidencial en el inventario de activos de información o en el marco de la ley colombiana vigente.
11. El correo electrónico institucional en sus mensajes debe contener una sentencia de confidencialidad, que será diseñada por la Oficina Asesora de Planeación y Sistemas y debe reflejarse en todos los buzones con dominio @insor.gov.co.
12. La divulgación de cifras o datos oficiales de la Entidad solo podrá ser emitida desde las direcciones de correo electrónico de la Dirección General, las subdirecciones, área de Comunicaciones y la Oficina Asesora de Planeación y Sistemas.
13. Está expresamente prohibido distribuir información del INSOR a través de correos personales o sitios web diferentes a los autorizados por la Oficina Asesora de Planeación y Sistemas.
14. El único servicio de correo electrónico autorizado para el manejo de la información institucional en la Entidad es el asignado por Oficina Asesora de Planeación y Sistemas, y que cuenta con el dominio @insor.gov.co, el cual cumple con todos los requerimientos técnicos y de Seguridad y Privacidad, evitando ataques de virus, spyware y otro tipo de software malicioso;

b) **Del uso de Internet:** La Oficina Asesora de Planeación y Sistemas establecerá políticas de navegación basadas en categorías y niveles de usuario por jerarquía y funciones, previa validación del eje de Seguridad y Privacidad de la Información. Para hacer efectivo el buen uso de los recursos de navegación de la Entidad, se deben tener en cuenta los siguientes lineamientos:

1. El uso del servicio de Internet está limitado exclusivamente para propósitos laborales.
2. Los servicios a los que un determinado usuario pueda acceder desde internet, dependerán del rol o funciones que desempeña el usuario en el INSOR y para los cuales esté formal y expresamente autorizado.
3. Todo usuario es responsable de informar a la Oficina Asesora de Planeación y Sistemas a través de la Mesa de Servicios – GLPI, los contenidos o acceso a servicios que no le estén autorizados y/o no correspondan a sus funciones dentro del INSOR.
4. Está expresamente prohibido el envío, y/o descarga, y/o visualización, de páginas con contenido insultante, ofensivo, injurioso, obsceno, violatorio de los derechos de autor y/o que atenten contra la integridad moral de las personas o instituciones.
5. Está expresamente prohibido el acceso a páginas web, portales, sitios web y/o aplicaciones web que no hayan sido autorizadas por el INSOR a través de la política de navegación.
6. Está expresamente prohibido el envío y/o descarga de cualquier tipo de software o archivos de fuentes externas, y/o de procedencia desconocida.
7. Está expresamente prohibida la propagación de virus o cualquier tipo de código malicioso.

El INSOR se reserva el derecho de monitorear los accesos, y por tanto el uso del servicio de internet de todos sus funcionarios o contratistas, además de limitar el acceso a determinadas páginas de Internet, los horarios de conexión, los servicios ofrecidos por la red, la descarga de archivos y cualquier otro ajeno a los fines de la Entidad;

c) **Del uso de los recursos tecnológicos:** Los recursos tecnológicos del INSOR, son herramientas de apoyo a las labores y responsabilidades de los funcionarios y contratistas. Por ello, su uso está sujeto a las siguientes directrices:

1. Los bienes de cómputo se emplearán de manera exclusiva y bajo la completa responsabilidad por el funcionario y/o contratista al cual le fueron asignados, y únicamente para el correcto desempeño de las funciones del cargo o las obligaciones. Por tanto, no pueden ser utilizados con fines personales o por terceros, no autorizados ante la Oficina Asesora de Planeación y Sistemas, mediante solicitud formal por los Directores, Subdirectores, Jefes de Oficina o Coordinadores de Grupos del INSOR a través de la Mesa de Servicios - GLPI.
2. Solo está permitido el uso de software licenciado por la Entidad y/o aquel que sin requerir licencia sea expresamente autorizado por la Oficina Asesora de Planeación y Sistemas. Las aplicaciones generadas o adquiridas por el INSOR, en desarrollo de su operación institucional, deben ser reportadas a la Oficina Asesora de Planeación y Sistemas, para su administración.
3. Es responsabilidad de los funcionarios y contratistas mantener copias de seguridad de la información contenida en sus estaciones de trabajo y entregarlas al INSOR en custodia al finalizar la vinculación con la Entidad.
4. Los usuarios no deben mantener almacenados en los discos duros de las estaciones cliente o discos virtuales de red, archivos de video, música y fotos que no sean de carácter institucional.
5. No está permitido fumar, ingerir alimentos o bebidas en el área de trabajo donde se encuentren los elementos tecnológicos.

6. No está permitido realizar conexiones o derivaciones eléctricas que pongan en riesgo la disponibilidad de la información por fallas en el suministro eléctrico a los equipos de cómputo.
7. Los únicos autorizados para hacer modificaciones o actualizaciones en los elementos y recursos tecnológicos, como destapar, agregar, desconectar, retirar, revisar y/o reparar sus componentes, son los designados por la Oficina Asesora de Planeación y Sistemas para tal labor.
8. La Oficina Asesora de Planeación y Sistemas realizará monitoreo sobre los dispositivos de almacenamientos externos, con el fin de prevenir o detectar fuga de información.
9. La única dependencia autorizada para trasladar los elementos y recursos tecnológicos de un puesto a otro es el Grupo de Servicios Administrativos, con el fin de llevar el control individual de inventarios. En tal virtud, toda reasignación de equipos deberá ajustarse a los procedimientos y competencias de dicha área.
10. La pérdida o daño de elementos o recursos tecnológicos, o de alguno de sus componentes, debe ser informada de inmediato al Grupo de Servicios Administrativos por el funcionario o contratista a quien se le hubiere asignado.
11. La pérdida de información debe ser informada con el detalle de la información extraviada a la Oficina Asesora de Planeación y Sistemas a través de la Mesa de Servicios- GLPI, como incidente de seguridad de la información.
12. Todo incidente de seguridad que comprometa la disponibilidad, integridad o confidencialidad de la información debe ser reportado con el procedimiento establecido a la Mesa de Servicios -GLPI a la mayor brevedad posible.
13. La Oficina Asesora de Planeación y Sistemas es la única dependencia autorizada para la administración del software, el cual no debe ser copiado, suministrado a terceros o utilizado para fines personales.
14. Todo acceso a la red de la Entidad mediante elementos o recursos tecnológicos no institucionales deberá ser informado, autorizado y controlado por la Oficina Asesora de Planeación y Sistemas.
15. Los equipos deben quedar apagados cada vez que el funcionario o contratista no se encuentre en la oficina durante la noche, esto es, con el fin de proteger la Seguridad y Privacidad y distribuir bien los recursos de la Entidad, siempre y cuando no vaya a realizar actividades vía remota.

d) **Del uso de los sistemas o herramientas de información:** Todos los funcionarios y contratistas del INSOR son responsables de la protección de la información que acceden y/o procesan y de evitar su pérdida, alteración, destrucción y/o uso indebido, para lo cual se dictan los siguientes lineamientos:

1. Las credenciales de acceso a la red y/o recursos informáticos (Usuario y Clave) son de carácter estrictamente personal e intransferible; los funcionarios y contratistas no deben revelar estas a terceros, ni utilizar claves ajenas.
2. Todo funcionario y/o contratista es responsable del cambio periódico de clave de acceso a los sistemas de información o recursos informáticos.
3. Todo funcionario y/o contratista es responsable de los registros y/o modificaciones de información que se hagan a nombre de su cuenta de usuario, toda vez que la clave de acceso es de carácter personal e intransferible.
4. En ausencia del funcionario y/o contratista, el acceso a la estación de trabajo le será bloqueada con una solicitud a Oficina asesora de Planeación y Sistemas a través de la Mesa de Servicios - GLPI, con el fin de evitar la exposición de la información y el acceso a terceros, que puedan generar daño, alteración o uso indebido, así como a la suplantación de identidad. El Grupo de Talento Humano debe reportar a la Oficina Asesora de Planeación y Sistemas cualquier tipo de novedad de los funcionarios y el Área de Contratación o el Supervisor del Contrato las novedades de los contratistas.

5. Cuando un funcionario o contratista cesa en sus funciones o culmina la ejecución de contrato con el INSOR, todos los privilegios sobre los recursos informáticos otorgados le serán suspendidos inmediatamente. La información del empleado y/o contratista serán almacenados en un repositorio de los servidores de la Entidad.
6. Cuando un funcionario o contratista cesa en sus funciones o culmina la ejecución de contrato con el INSOR, el supervisor o jefe inmediato es el encargado de la custodia de los recursos de información, incluyendo la cesión de derechos de propiedad intelectual de acuerdo con la normativa vigente.
7. Todos los funcionarios y contratistas de la Entidad deben respetar lo estipulado en la Ley 23de 1982 *"Sobre derechos de autor"*, la Decisión número 351 de 1993 de la Comunidad Andina de Naciones, así como cualquier otra que adicione, modifique o reglamente la materia.

ARTÍCULO 9°. POLÍTICA DE CONTROL DE ACCESO. Los propietarios de los activos deben establecer medidas de control de acceso a nivel de red, sistema operativo, sistemas de información y servicios de tecnologías de la información con el fin de mitigar riesgos asociados al acceso a la información y servicios de infraestructura tecnológica de personal no autorizado, salvaguardando la integridad, disponibilidad y confidencialidad de la información del INSOR.

ARTÍCULO 10. POLÍTICA DE CRIPTOGRAFÍA. La Oficina Asesora de Planeación y Sistemas deberá asegurar el uso adecuado y efectivo de la criptografía para proteger la confidencialidad, integridad y disponibilidad de la información.

ARTÍCULO 11. POLÍTICA DE SEGURIDAD FÍSICA Y DEL ENTORNO. El INSOR debe garantizar la protección del perímetro de seguridad de las instalaciones físicas, controlar el acceso del personal y la permanencia en las oficinas e instalaciones, así como controlar el acceso a áreas restringidas (áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones.). Además, mitigar los riesgos y amenazas externas y ambientales, con el fin de garantizar la confidencialidad, disponibilidad e integridad de la información de la Entidad.

Todos los funcionarios, contratistas y visitantes que se encuentren en las instalaciones físicas del INSOR, deben estar debidamente identificados con un documento que acredite su tipo de vinculación, el cual se debe portar en un lugar visible.

a) Los visitantes del INSOR, siempre deben permanecer acompañados por un funcionario o contratista debidamente identificado.
b) El personal de empresas contratistas que desempeñen las funciones de forma permanente en las instalaciones del INSOR, deben estar identificados con chalecos o distintivos del Contratista y portar el carné de la ARL.

ARTÍCULO 12. POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LAS OPERACIONES. La Oficina Asesora de Planeación y Sistemas, será la encargada de la operación y administración de los recursos tecnológicos que soportan la operación del INSOR. Así mismo, velará por la eficiencia de los controles asociados a los recursos tecnológicos protegiendo la confidencialidad, integridad y disponibilidad de la información. Igualmente, se encargará de asegurar que los cambios efectuados sobre los recursos tecnológicos, sean controlados y debidamente autorizados. De igual manera, deberá proveer la capacidad de procesamiento requerida en los recursos tecnológicos y sistemas de información del INSOR, efectuando proyecciones de crecimiento y provisiones en la plataforma tecnológica de acuerdo al crecimiento de la Entidad.

La Oficina Asesora de Planeación y Sistemas debe realizar y mantener copias de seguridad de la información de la Entidad en medio digital, siempre que esta sea reportada por el responsable de la misma, con el objetivo de recuperarla en caso de cualquier tipo de falla, ya sea de hardware, software, o de procedimientos operativos al interior de la Entidad. Para estos efectos, la Oficina Asesora de Planeación y Sistemas realizará la copia respectiva, de acuerdo con el esquema definido previamente en el documento Procedimiento Gestión Copias de Seguridad de la Entidad, el cual debe ser diseñado esta dependencia y en conjunto con los líderes de Proceso.

ARTÍCULO 13. POLÍTICA DE SEGURIDAD DE LAS COMUNICACIONES. La Oficina Asesora de Planeación y Sistemas, establecerá los mecanismos necesarios para proveer la disponibilidad de las redes y de los servicios que dependen de ellas y dispondrá y monitoreará los mecanismos necesarios de Seguridad y Privacidad para proteger la integridad y la confidencialidad de la información del INSOR.

PARÁGRAFO. Como parte de sus términos y condiciones iniciales de trabajo, los funcionarios y/o contratistas, cualquiera sea su nivel jerárquico dentro de la entidad, firmarán un Compromiso de Confidencialidad o no divulgación, en lo que respecta al tratamiento de la información de la entidad, en los términos de la Ley 1581 de 2012, así como el Capítulo 25 del Decreto número 1074 de 2015 y la Ley 1712 de 2014 reglamentada por el Capítulo 2 del Decreto número 1081 de 2015 y las demás normas que las adicionen, modifiquen, reglamenten o complementen. El documento original de dicho compromiso deberá ser retenido en forma segura por el grupo de Talento Humano o el área de Contratación, según el caso, si tal compromiso de confidencialidad de la información no estuviere incluido como una cláusula del respectivo contrato o en el Acta de Posesión del Servidor. Así mismo, mediante el Compromiso de Confidencialidad el Servidor o el contratista, declarará conocer y aceptar la existencia de determinadas actividades que pueden ser objeto de control y monitoreo. Estas actividades deben ser detalladas a fin de no violar el derecho a la privacidad, ni los derechos del servidor o contratista.

En el caso de que sea personal que ejecute tareas propias del INSOR y haya sido contratado en el marco de un contrato o convenio con el INSOR, debe reposar en la carpeta de ejecución del contrato un compromiso de confidencialidad firmado entre el INSOR (Supervisor del Contrato) y el representante legal.

ARTÍCULO 14. POLÍTICA DE SEGURIDAD PARA LA ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS. La Oficina Asesora de Planeación y Sistemas velará porque el desarrollo interno o externo de los sistemas de información, cumpla con los requerimientos de Seguridad y Privacidad adecuados para la protección de la información del INSOR.

La Oficina Asesora de Planeación y Sistemas será la única dependencia de la Entidad con la capacidad de adquirir, desarrollar o avalar la adquisición y recepción de software de cualquier tipo, conforme a los requerimientos de las diferentes dependencias, con el fin de garantizar la conveniencia, soporte, mantenimiento y seguridad de la información de los sistemas que operan en el Instituto. En consecuencia, cualquier software que opere en el INSOR y no haya sido entregado a la Oficina Asesora de Planeación y Sistemas, no serán responsabilidad de la misma, no se le podrá brindar soporte y no se le podrá salvaguardar la información.

ARTÍCULO 15. POLÍTICA DE SEGURIDAD Y PRIVACIDAD PARA RELACIÓN CON PROVEEDORES. El INSOR establecerá mecanismos de control en relaciones con sus proveedores, teniendo en cuenta que se debe asegurar la información a la que tengan acceso, supervisando el cumplimiento de lo establecido en el Eje de seguridad de la información. Los Supervisores de los contratos o convenios en conjunto con la

Oficina Asesora de Planeación y Sistemas, tendrán la responsabilidad de la divulgación de las políticas y procedimientos de la Seguridad y Privacidad de la información.

ARTÍCULO 16. POLÍTICA DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN. El INSOR promoverá entre los funcionarios y contratistas el reporte de incidentes relacionados con la seguridad de la información y sus medios, reporte y seguimiento. Así mismo, asignará responsables para el tratamiento de los incidentes de Seguridad y Privacidad de la información, quienes tendrán la responsabilidad de investigar y solucionar los incidentes reportados, de acuerdo con su criticidad. la Direccion General o a quien éste delegue, son los únicos autorizados para reportar incidentes de seguridad ante las autoridades. Así mismo, son los únicos canales de comunicación autorizados para hacer pronunciamientos oficiales ante entidades externas, medios de comunicación o la ciudadanía.

ARTÍCULO 17. POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN EN LA CONTINUIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN. El INSOR dispondrá los planes necesarios para la implementación del proceso de continuidad de la operación desde el punto de vista tecnológico, el cual será operado según el caso por la Oficina Asesora de Planeación y Sistemas, la cual deberá garantizar la redundancia de los sistemas de información de carácter misional, y en los servicios de sitio web institucional, telefonía IP y correo electrónico institucional. Además, la infraestructura tecnológica necesaria para soportarlos y garantizar la continuidad de la operación para el cumplimiento de sus obligaciones.

ARTÍCULO 18. POLÍTICA DE CUMPLIMIENTO. El INSOR velará por la identificación, documentación y cumplimiento de los requisitos legales enmarcados en la Seguridad y Privacidad de la información del Estado colombiano, entre ella la referente a derechos de autor y propiedad intelectual, protección de datos personales y ley de transparencia y del derecho de acceso a la información pública nacional y las consignadas en los normogramas del INSOR.

CAPÍTULO III.

REVISIÓN, VIGENCIA Y DEROGATORIA.

ARTÍCULO 19. REVISIÓN. La Política de Seguridad y Privacidad de la Información será revisada semestralmente, o antes si existiesen modificaciones que así lo requieran, para garantizar que sigue siendo oportuna, suficiente y eficaz. Este proceso será liderado por la Oficina Asesora de Planeación y Sistemas y aprobado por el Comité de Desarrollo Administrativo y Control.

ARTÍCULO 20. VIGENCIA Y DEROGATORIA. La presente resolución rige a partir de la fecha de su publicación.

COMUNÍQUESE, PUBLÍQUESE Y CÚMPLASE

Dada en Bogotá, D. C., a los 05 DIC 2016

OLGA MARCELA CUBIDES SALAZAR
Directora General

Elaboró: Jhon Mayorga- Contratista
Revisó: Pablo Antonio Ordoñez- Secretario General
Carolina Villamil – Jefe Oficina Asesora Jurídica
Aprobó: Orlando Castillo León