RESOLUCIÓN No. 9364 **13 SEP 2016**

Por la cual se actualiza la Política de Seguridad de la Información, se definen lineamientos frente su uso y manejo y se deroga una resolución

LA DIRECTORA GENERAL DEL INSTITUTO COLOMBIANO DE BIENESTAR FAMILIAR CECILIA DE LA FUENTE DE LLERAS

En uso de sus facultades legales y estatutarias señaladas en las Leyes 7ª de 1979, 87 de 1993, el artículo 78 de la Ley 489 de 1998 y el artículo 2.2.9.1.2.3 del Decreto 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 ICBF mediante Resolución No. 10232 de 2015, reorganizó el Sistema Integrado de Gestión y asignó roles y responsabilidades en los ejes que lo integran, siendo la Seguridad de la Información uno de ellos.

Que el Decreto 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 2.2.9.1.2.1 como 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 mediante la Resolución No. 10806 del 11 de diciembre de 2015, el ICBF adoptó la Política de Seguridad de la Información y definió 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 mediante la Resolución No. 8080 del 11 de agosto de 2016, por la cual se aprobó el Manual del Sistema Integrado de Gestión, se adoptó el modelo de operación por proceso del ICBF; del cual hacen parte el Manual de Seguridad de la Información y la Declaración de Aplicabilidad.

Que en sesión virtual Comité SIGE realizada el 27 de julio de 2016 se aprobó la actualización de la política general de Seguridad de la Información, además se identificaron una serie de aspectos que deben ser adicionados y ajustados para garantizar que continúe siendo oportuna, suficiente y eficiente, siendo necesario actualizarla.

Que, en mérito de lo expuesto,

RESUELVE

CAPÍTULO I.
DISPOSICIONES GENERALES.

RESOLUCIÓN No. 9364 13 SEP 2016

Por la cual se actualiza la Política de Seguridad de la Información, se definen lineamientos frente su uso y manejo y se deroga una resolución

ARTÍCULO PRIMERO. Objeto. La presente resolución tiene como objeto la actualización de la política general de seguridad de la información del Instituto Colombiano de Bienestar Familiar, así como definir lineamientos frente a su uso y manejo.

ARTÍCULO SEGUNDO. Política de Seguridad de la Información. El ICBF 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 de la Información, con la finalidad de prestar servicios con calidad y transparencia a la primera infancia, la niñez, la adolescencia y el bienestar de las familias Colombianas.

ARTÍCULO TERCERO. Ámbito de Aplicación. Lo contenido en esta política de Seguridad de la Información, aplica donde el Instituto Colombiano de Bienestar Familiar - ICBF tenga presencia o desarrolle su acompañamiento a través de la recolección, procesamiento, almacenamiento, recuperación, intercambio y consulta de información, con personal interno o externo, en el desarrollo de la misión institucional y cumplimiento de sus objetivos estratégicos.

ARTÍCULO CUARTO. Objetivos.

1. Brindar mecanismos de aseguramiento para el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información del ICBF.
2. Mitigar los incidentes de Seguridad de la Información en el ICBF.
3. Establecer los lineamientos necesarios para el manejo de la información y los recursos tecnológicos del ICBF.
4. Gestionar los riesgos de seguridad de la información.

CAPÍTULO II.
POLÍTICAS GENERALES DE MANEJO DE INFORMACIÓN.

ARTÍCULO QUINTO. Tratamiento de la Información. Para el tratamiento de la información de los niños, niñas, adolescentes, familias y comunidades colombianas a las cuales se les presta el acompañamiento en el marco del mandato legal encargado por el Gobierno Nacional al ICBF, así como la información de los servidores públicos y colaboradores que participan en el desarrollo de las funciones de dicho mandato, el ICBF cuenta con la "*Política de Tratamiento de Datos Personales del Instituto Colombiano de Bienestar Familiar*" dando cumplimiento con 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 1074 de 2015, la Ley 1712 de 2014, reglamentada por el Capítulo 2 del Título 1 de la Parte 1 del Decreto 1081 de 2015, y las demás normas externas o internas que los modifiquen, adicionen o complementen.

ARTÍCULO SEXTO. Política de Seguridad de los Recursos Humanos. El ICBF a través de la Dirección de Gestión Humana debe propender que los servidores públicos 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. La Dirección de Contratación deberá incluir en las minutas de los contratistas cualquiera que sea su modalidad, las cláusulas u obligaciones correspondientes 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.

ARTÍCULO SÉPTIMO. Política de Gestión de Activos. El Instituto Colombiano de Bienestar Familiar a través de la Dirección de Información y Tecnología, 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 ICBF 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 ICBF, discriminado por procesos, regionales y Centros Zonales, de acuerdo a la misma Guía para Desarrollo de Inventario y Clasificación de Activos.

   Con el objetivo implantar los controles de seguridad, las dependencias que tienen la custodia de la información generada en el marco de su función, se encargarán 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:** La Dirección Administrativa a través del grupo de gestión documental y con el acompañamiento del eje de Seguridad de la Información, deben implementar los controles necesarios para que los archivos de gestión cuenten con los mecanismos de seguridad con el fin de proteger y conservar la confidencialidad, integridad y disponibilidad de la información del ICBF.

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

ARTÍCULO OCTAVO. Responsabilidades de los Colaboradores frente al uso de los Recursos Tecnológicos. Todos los colaboradores que hagan uso de los activos de información del ICBF, tienen la responsabilidad de cumplir las políticas establecidas para el uso aceptable de los activos de información, entendiendo que el uso no adecuado de los recursos puede poner en riesgo la continuidad de la misión institucional.

a. **Del 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 ICBF, con los siguientes lineamientos:

   - 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.
   - 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.
   - 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 estos.
   - Está prohibido el envío de correos masivos (más de 150 destinatarios) a nivel nacional tanto internos como externos, salvo a través de la Dirección General, Subdirección General, Secretaría General, Oficina Asesora de Comunicaciones, Dirección de Planeación y Gestión de Control, Dirección de Gestión Humana y Dirección de Información y Tecnología.

- En las sedes regionales está prohibido el envío de correos masivos (más de 20 destinatarios) tanto interno como externo, salvo a través de los Directores Regionales y Coordinadores de la Regional y Centro Zonal.
- Todo mensaje SPAM o CADENA debe ser inmediatamente reportado a la Dirección de Información y Tecnología a través de la Mesa de Servicios como incidente de seguridad de la información según procedimiento establecido. No está permitido el envío y/o reenvío de mensajes en cadena.
- Todo mensaje sospechoso respecto de su remitente o contenido debe ser inmediatamente reportado a la Dirección de Información y Tecnología a través de la Mesa de Servicios, como incidente de seguridad de la información según procedimiento establecido y proceder de acuerdo a las indicaciones de esta Dirección, 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).
- 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 de la Entidad.
- 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.
- Está expresamente prohibido distribuir información del ICBF no pública, a otras entidades o ciudadanos sin la debida autorización de la Dirección General, Subdirección General y/o Dirección de Planeación y Control de Gestión.
- 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.
- El correo electrónico institucional en sus mensajes debe contener una sentencia de confidencialidad, que será diseñada por la Dirección de Información y Tecnología a través de la Subdirección de Recursos Tecnológicos y debe reflejarse en todos los buzones con dominio @icbf.gov.co.
- La divulgación de cifras o datos oficiales de la Entidad sólo podrá ser emitida desde las direcciones de correo electrónico de la Dirección General, Subdirección General, Oficina Asesora de Comunicaciones y la Dirección de Planeación y Control de Gestión.
- Está expresamente prohibido distribuir información del ICBF a través de correos personales o sitios web diferentes a los autorizados por la Dirección de Información y Tecnología.
- El único servicio de correo electrónico autorizado para el manejo de la información institucional en la Entidad es el asignado por la Dirección de Información y Tecnología, y que cuenta con el dominio @icbf.gov.co, el cual cumple con todos los requerimientos técnicos y de seguridad, evitando ataques de virus, spyware y otro tipo de software malicioso.

b. **Del Uso de Internet:** La Dirección de Información y Tecnología a través de la Subdirección de Recursos Tecnológicos establecerá políticas de navegación basadas en categorías y niveles de usuario por jerarquía y funciones, previa validación del eje de Seguridad de la Información.

De acuerdo al buen uso de los recursos de navegación de la Entidad se deben tener en cuenta los siguientes lineamientos:

- El uso del servicio de Internet está limitado exclusivamente para propósitos laborales.

- Los servicios a los que un determinado usuario pueda acceder desde internet dependerán del rol o funciones que desempeña el usuario en el ICBF y para los cuales esté formal y expresamente autorizado.
- Todo usuario es responsable de informar a la Dirección de Información y Tecnología a través de la Mesa de Servicios los contenidos o acceso a servicios que no le estén autorizados y/o no correspondan a sus funciones dentro del ICBF.
- 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.
- Está expresamente prohibido el acceso a páginas web, portales, sitios web y/o aplicaciones web que no hayan sido autorizadas por el ICBF a través de la política de navegación.
- Está expresamente prohibido el envío y/o descarga de cualquier tipo de software o archivos de fuentes externas, y/o de procedencia desconocida.
- Está expresamente prohibida la propagación de virus o cualquier tipo de código malicioso.

El ICBF 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 ICBF, son herramientas de apoyo a las labores y responsabilidades de los funcionarios y contratistas. Por ello, su uso está sujeto a las siguientes directrices:

- Los bienes de cómputo se emplearán de manera exclusiva y bajo la completa responsabilidad por el funcionario y contratista al cual han sido 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 Dirección de Información y Tecnología mediante solicitud formal por los Directores, Subdirectores, Jefes de Oficina o Coordinadores de Grupos del ICBF a través de la Mesa de Servicios.
- Sólo está permitido el uso de software licenciado por la Entidad y/o aquel que sin requerir licencia sea expresamente autorizado por la Dirección de Información y Tecnología a través de la Subdirección de Recursos tecnológicos. Las aplicaciones generadas o adquiridas por el ICBF, en desarrollo de su operación institucional, deben ser reportadas a la Dirección de Información y Tecnología a través de la Subdirección de Sistemas Integrados de Información, para su administración.
- Es responsabilidad de los funcionarios y contratistas mantener copias de seguridad de la información contenida en sus estaciones de trabajo y entregarlas al ICBF en custodia al finalizar la vinculación con la Entidad.
- 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.
- No está permitido fumar, ingerir alimentos o bebidas en el área de trabajo donde se encuentren los elementos tecnológicos.
- 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.
- 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 Dirección de Información y Tecnología a través de la Subdirección de Recursos Tecnológicos para tal labor.

- La Dirección de Información y Tecnología a través de la Subdirección de Recursos Tecnológicos realizará monitoreo sobre los dispositivos de almacenamientos externos, con el fin de prevenir o detectar fuga de información.
- La única dependencia autorizada para trasladar los elementos y recursos tecnológicos de un puesto a otro es la Dirección Administrativa, 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 dependencia.
- La pérdida o daño de elementos o recursos tecnológicos, o de alguno de sus componentes, debe ser informada de inmediato a la Dirección Administrativa por el funcionario o contratista a quien se le hubiere asignado.
- La pérdida de información debe ser informada con el detalle de la información extraviada a la Dirección de Información y Tecnología a través de la Mesa de Servicios como incidente de seguridad de la información.
- 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 a la mayor brevedad posible.
- La Dirección de Información y Tecnologías es la única dependencia autorizada para la administración del software, el cual no debe ser copiado, suministrado a terceros o utilizado para fines personales.
- Todo acceso a la red de la Entidad mediante elementos o recursos tecnológicos no institucionales deberá ser informado, autorizado y controlado por la Dirección de Información y Tecnología a través de la Subdirección de Recursos Tecnológicos.
- 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 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 ICBF 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:

- 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 éstas a terceros ni utilizar claves ajenas.
- Todo funcionario y contratista es responsable del cambio de clave de acceso a los sistemas de información o recursos informáticos periódicamente.
- Todo funcionario y 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.
- En ausencia del funcionario y/o contratista, el acceso a la estación de trabajo le será bloqueada con una solicitud a la Dirección de Información y Tecnología a través de la Mesa de Servicios, 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. La Dirección de Gestión Humana debe reportar cualquier tipo de novedad de los funcionarios y la Dirección de Contratación o el Supervisor del Contrato las novedades de los contratistas.
- Cuando un funcionario o contratista cesa en sus funciones o culmina la ejecución de contrato del ICBF, 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.

- Cuando un funcionario o contratista cesa en sus funciones o culmina la ejecución de contrato del ICBF, 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 a la normativa vigente.
- Todos los funcionarios y contratistas de la Entidad deben respetar lo estipulado en la Ley 23 de 1982 "*Sobre derechos de autor*", la Decisión 351 de 1993 de la Comunidad Andina de Naciones, así como cualquier otra que adicione, modifique o reglamente la materia.

ARTÍCULO NOVENO. 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 ICBF.

ARTÍCULO DÉCIMO. Política de Criptografía. La Dirección de Información y Tecnología deberá asegurar el uso adecuado y efectivo de la criptografía para proteger la confidencialidad, integridad y disponibilidad de la información.

ARTÍCULO DÉCIMO PRIMERO. Política de Seguridad Física y del Entorno. El ICBF 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 ICBF deben estar debidamente identificados, con un documento que acredite su tipo de vinculación y se debe portar en un lugar visible.

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

ARTÍCULO DÉCIMO SEGUNDO. Política de Seguridad de las Operaciones. La Dirección de Información y Tecnología a través de la Subdirección de Recursos Tecnológicos será la encargada de la operación y administración de los recursos tecnológicos que soportan la operación del ICBF, así mismo, velará por la eficiencia de los controles asociados a los recursos tecnológicos protegiendo la confidencialidad, integridad y disponibilidad de la información, así como, la de asegurar que los cambios efectuados sobre los recursos tecnológicos, serán controlados y debidamente autorizados. De igual manera, deberá proveer la capacidad de procesamiento requerida en los recursos tecnológicos y sistemas de información del ICBF, efectuando proyecciones de crecimiento y provisiones en la plataforma tecnológica de acuerdo al crecimiento de la Entidad.

La Dirección de Información y Tecnología a través de la Subdirección de Recursos Tecnológicos debe realizar y mantener copias de seguridad de la información de la Entidad en medio digital, siempre que ésta 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.

Se efectuará 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 por la Subdirección de Recursos Tecnológicos, en conjunto con los líderes de Proceso.

ARTÍCULO DÉCIMO TERCERO. Política de Seguridad de las Comunicaciones. La Dirección de Información y Tecnología a través de la Subdirección de Recursos Tecnológicos, establecerá los mecanismos necesarios para proveer la disponibilidad de las redes y de los servicios que dependen de ellas; así mismo, dispondrá y monitoreará los mecanismos necesarios de seguridad para proteger la integridad y la confidencialidad de la información del ICBF.

PARÁGRAFO. Como parte de sus términos y condiciones iniciales de trabajo, los funcionarios 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 1074 de 2015 y la Ley 1712 de 2014 reglamentada por el capítulo 2 del Decreto 1081 de 2015 y las demás normas que las adicionen, modifiquen, reglamenten o complementen. Dicho compromiso (documento original) deberá ser retenido en forma segura por la Dirección de Gestión Humana o la Dirección 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 funcionario. Así mismo, mediante el Compromiso de Confidencialidad el funcionario 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 funcionario o contratista.

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

ARTÍCULO DÉCIMO CUARTO. Política de Seguridad para la Adquisición, Desarrollo y Mantenimiento de Sistemas. La Dirección de Información y Tecnología a través de la Subdirección de Sistemas Integrados de información velará porque el desarrollo interno o externo de los sistemas de información cumpla con los requerimientos de seguridad adecuados para la protección de la información del ICBF.

La Dirección de Información y Tecnología 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 Instituto y no haya sido entregado a la Dirección de Información y Tecnología, no serán responsabilidad de la misma, no se le brindará soporte y no se le salvaguardará la información.

ARTÍCULO DÉCIMO QUINTO. Política de Seguridad para Relación con Proveedores. El ICBF 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 Dirección de Información y Tecnología, tendrán la responsabilidad de la divulgación de las políticas y procedimientos de la seguridad de la información.

ARTÍCULO DÉCIMO SEXTO. Política de Gestión de Incidentes de Seguridad de la Información. El ICBF 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 de la información, quienes tendrán la responsabilidad de investigar y solucionar los incidentes

reportados, de acuerdo con su criticidad. El Director 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 DÉCIMO SÉPTIMO. Política de Seguridad de la Información en la Continuidad de las Tecnologías de la Información. El ICBF 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 Dirección de Información y Tecnología, la cual deberá garantizar la redundancia de los sistemas de información de carácter misional (SIM y CUENTAME), y en los servicios de sitio web institucional, telefonía IP y correo electrónico institucional; además, la infraestructura tecnológica necesaria para soportarlos, en la Sede Dirección General, con el fin de garantizar la continuidad de la operación para el cumplimiento de mandato legal.

ARTÍCULO DÉCIMO OCTAVO. Política de Cumplimiento. El ICBF velará por la identificación, documentación y cumplimiento de los requisitos legales enmarcados en la seguridad 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 la Matriz de Requisitos Legales del ICBF.

PARÁGRAFO. Todas las políticas contenidas en el Capítulo II de éste acto administrativo se encuentran reglamentadas por los lineamientos contenidos como anexo al Manual del Sistema Integrado de Gestión del ICBF, el cual es parte integral de este documento.

CAPÍTULO III.
REVISIÓN, VIGENCIA Y DEROGATORIA.

ARTÍCULO DÉCIMO NOVENO. Revisión. La Política de Seguridad 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 Dirección de Información y Tecnología, y revisados por el Comité SIGE.

ARTÍCULO VIGÉSIMO. Vigencia y Derogatoria. La presente Resolución rige a partir de la fecha de su publicación y deroga la resolución 10806 de 2015, así como las demás disposiciones que le sean contrarias.

PUBLÍQUESE, COMUNÍQUESE Y CÚMPLASE
Dada en Bogotá, D.C., a los

13 SEP 2016

CRISTINA PLAZAS MICHELSEN
Directora General

Elaboró: Andrés Díaz Molina – Dirección de Información y Tecnología
Revisó: María Alexandra Lugo, César Augusto Mejía – Oficina Asesora Jurídica
Aprobó: María Teresa Salamanca – Jefe Oficina Asesora Jurídica (E)
Piedad Cecilia Montero Villegas - Dirección Información y Tecnología
Juan Carlos Bolivar López - Dirección de Planeación y Control de Gestión