RESOLUCIÓN No. 3600 **2 2 MAY 2017**

Por la cual se modifica la Resolución No. 9364 de 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, 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 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 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. 9364 de 2016, el ICBF actualizó 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 dentro de la revisión realizada a la política de Seguridad de la Información conforme a lo dispuesto en el artículo décimo noveno de la precitada resolución, se encontró la necesidad de actualizarla debido a que se incluyen apartados concerniente a recursos tecnológicos, revisión de la misma y componente de información.

Que es necesario modificar la Resolución No. 9364 de 2016 ajustando la Política de Seguridad de la Información para garantizar que siga siendo oportuna, eficaz y eficiente.

Que, en mérito de lo expuesto,

RESUELVE

CAPÍTULO I.
DISPOSICIONES GENERALES.

ARTÍCULO PRIMERO. Modifíquese el artículo 8º de la Resolución No. 9364 de 2016, el cual quedará así:

RESOLUCIÓN No. 3600 22 MAY 2017

Por la cual se modifica la Resolución No. 9364 de 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 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.), la cual 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 internos como externos, salvo a través de los Directores Regionales, así como Coordinadores Regionales y de 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 dicha Dirección; lo anterior, debido a que puede ser contentivo de virus, en especial si contiene archivos adjuntos con extensiones .exe, .bat, .prg, .bak, .pif, o tenga 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 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, a otras entidades o ciudadanos sin la debida autorización de Director(a) General, Directores Regionales, Subdirector(a) General, Directores Misionales y/o Director(a) 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 clasificada o reservada 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, Direcciones Regionales, 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 o transmisión 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 en el ICBF y para las 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, 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 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 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 o contratista al cual han sido asignados, y únicamente para el desempeño de las funciones del cargo o las obligaciones contractuales pactadas. 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.*
- *En caso que el colaborador deba hacer uso de equipos ajenos al ICBF, estos deberán cumplir con la legalidad del Software instalado, antivirus actualizado y no podrá conectarse directamente a la red del ICBF, sino que deberá hacerlo a través de red de visitante utilizando una VPN suministrada por la Entidad. Estas condiciones deben ser verificadas por los ingenieros de la Subdirección de Recursos Tecnológicos a nivel Central, Regional o Zonal.*
- *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 computadores de escritorio, portátiles 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 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 como USB, CD-ROM, Discos Duros externos, entre otros, 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 o quien haga sus veces en el nivel regional y zonal, 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 detalle a la Dirección de Información y Tecnología a través de la Mesa de Servicios como incidente de seguridad.*
- *Todo incidente de seguridad que comprometa la disponibilidad, integridad o confidencialidad de la información debe ser reportado a la mayor brevedad posible a la Mesa de Servicios, siguiendo el procedimiento establecido.*
- *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 ni 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 o durante la noche, esto, 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, así como de evitar su pérdida, alteración, destrucción y uso indebido, para lo cual se dictan los siguientes lineamientos:*

- *Las credenciales de acceso a la red y a los recursos informáticos (Usuario y Clave) son de carácter estrictamente personal e intransferible; los funcionarios y contratistas no deben revelarlas 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 modificaciones de información que se hagan a nombre de su cuenta de usuario.*

RESOLUCIÓN No. 3630 22 MAY 2017

Por la cual se modifica la Resolución No. 9364 de 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"

- *En ausencia del funcionario 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 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 SEGUNDO. Modifíquese el artículo 9º de la Resolución No. 9364 de 2016, el cual quedará así:

ARTÍCULO NOVENO. Política de Control de Acceso. *Los propietarios de los activos de información deben establecer medidas de control de acceso a nivel de red, sistema operativo, sistemas de información, servicios de tecnologías de la información e infraestructura física 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 TERCERO. Modifíquese el artículo 10º de la Resolución No. 9364 de 2016, el cual quedará así:

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

ARTÍCULO CUARTO. Modifíquese el artículo 11 de la Resolución No. 9364 de 2016, el cual quedará así:

ARTÍCULO DÉCIMO PRIMERO. Política de Seguridad Física y del Entorno. *El ICBF debe contar con controles para 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*

RESOLUCIÓN No. 3600 22 MAY 2017

Por la cual se modifica la Resolución No. 9364 de 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"

y ambientales, con el fin de evitar afectación la confidencialidad, disponibilidad e integridad de la información de la Entidad.

***PARÁGRAFO 1.** 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.*

***PARÁGRAFO 2.** Los visitantes en el ICBF, siempre deben permanecer acompañados por un funcionario o contratista debidamente identificado.*

***PARÁGRAFO 3.** El personal de empresas contratistas que desempeñen 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 QUINTO. Modifíquese el artículo 13 de la Resolución No. 9364 de 2016, el cual quedará así:

***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 Tratamiento de Datos 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, la Dirección de Contratación o quien haga las veces en las Direcciones Regionales., según el caso, si tal acuerdo 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.*

***PARÁGRAFO 2.** 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 por el Representante Legal de la empresa contratista o con la cual se realiza el convenio.*

ARTÍCULO SEXTO. Modifíquese el artículo 17 de la Resolución No. 9364 de 2016, el cual quedará así:

***ARTÍCULO DÉCIMO SÉPTIMO. Política de Seguridad de la Información en la Continuidad de las Tecnologías de la Información.** El ICBF dispondrá los planes*

22 MAY 2017

RESOLUCIÓN No. 3630

Por la cual se modifica la Resolución No. 9364 de 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"

necesarios para la implementación del proceso de continuidad de la operación desde el punto de vista tecnológico, el cual será operado por la Dirección de Información y Tecnología, la cual deberá contar con redundancias 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 de la Dirección General, con el fin de ofrecer continuidad de la operación tecnológica en el cumplimiento del mandato legal.

ARTÍCULO SÉPTIMO. Modifíquese el artículo 19 de la Resolución No. 9364 de 2016, el cual quedará así:

ARTÍCULO DÉCIMO NOVENO. Revisión. *La Política de Seguridad de la Información será revisada anualmente, o antes si existiesen modificaciones que así lo requieran, para que se mantenga oportuna, suficiente y eficaz. Este proceso será liderado por la Dirección de Información y Tecnología, y revisados por el Comité SIGE.*

ARTÍCULO OCTAVO. Vigencia y Derogatoria. La presente Resolución rige a partir de la fecha de su publicación y modifica en lo pertinente la Resolución No. 9364 de 2016.

PUBLÍQUESE, COMUNÍQUESE Y CÚMPLASE
Dada en Bogotá, D.C., a los 22 MAY 2017

CRISTINA PLAZAS MICHELSEN
Directora General

Aprobó: Héctor Germán Páramo Urrea - Director de Información y Tecnología (e) / Juan Carlos Bolivar López - Director de Planeación y Control de Gestión / Luz Karime Fernandez – Jefe Oficina Asesora Jurídica
Revisó: Mónica Liliana Nieto / César Augusto Mejía – Oficina Asesora Jurídica
Elaboró: Andrés Díaz Molina – Dirección de Información y Tecnología