**RESOLUCIÓN No.**

*"Por la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información, y se derogan las Resoluciones 4286 de 2020 y 5515 de 2021"*

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

En uso de sus facultades legales y estatutarias y, en especial de las que le confieren la Ley 7 de 1979, la Ley 87 de 1993, el artículo 78 de la Ley 489 de 1998, el artículo 2.2.9.1.3.2 del Decreto 1078 de 2015, modificado por el Decreto 1008 de 2018 y,

**CONSIDERANDO:**

Que de acuerdo con lo preceptuado en el artículo 209 de la Constitución Política, *"La función administrativa está al servicio de los intereses generales y se desarrolla con fundamento en los principios de igualdad, moralidad, eficacia, economía, celeridad, imparcialidad y publicidad".*

Que la Constitución Política 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 el artículo 269 ibidem señala que, ***"****En las entidades públicas, las autoridades correspondientes están obligadas a diseñar y aplicar, según la naturaleza de sus funciones, métodos y procedimientos de control interno, de conformidad con lo que disponga la ley, la cual podrá establecer excepciones y autorizar la contratación de dichos servicios con empresas privadas colombianas."*

Que el Decreto 1078 de 2015, modificado por el Decreto 1008 de 2018, en el artículo 2.2.9.1.1.3. consagra la seguridad de la información como un principio de la Política de Gobierno Digital; el cual tiene como fin *"crear condiciones de uso confiable en el entorno digital, mediante un enfoque basado en la gestión de riesgos, preservando la confidencialidad, integridad y disponibilidad de la información de las entidades del Estado, y de los servicios que prestan al ciudadano."*

Que el artículo 2.2.9.1.2.1 ídem establece que, la Política de Gobierno Digital se desarrollará a través de componentes y habilitadores transversales, los cuales son los elementos fundamentales de Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales, que a su vez permiten el desarrollo y el logro de los propósitos de la Política mencionada.

Que el Consejo Nacional de Política Económica y Social – CONPES, en el marco de la ejecución del Documento CONPES 3995 del 1 de julio de 2020, estableció la Política Nacional de Confianza y Seguridad Digital.

Que mediante Resolución 4286 de 2020, el ICBF derogó la Resolución 9674 de 2018 y actualizó la Política de Seguridad de la Información y lineamientos frente a su uso y manejo; teniendo en cuenta la normativa vigente de protección de datos personales, así como de transparencia y acceso a la información. Esta, a su vez, fue modificada por la Resolución 5515 del 31 de agosto de 2021.

Que el Decreto 1083 de 2015, modificado por el Decreto 1499 de 2017, adoptó el Modelo Integrado de Planeación y Gestión - MIPG, definiéndolo en su artículo 2.2.22.3.2 como *"(…) un marco de referencia para dirigir, planear, ejecutar, hacer seguimiento, evaluar y controlar la gestión de las entidades y organismos públicos, con el fin de generar resultados que atiendan los planes de desarrollo y resuelvan las necesidades y problemas de los ciudadanos, con integridad y calidad en el servicio".*

**RESOLUCIÓN No.**

*"Por la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información, y se derogan las Resoluciones 4286 de 2020 y 5515 de 2021"*

Que el artículo 2.2.22.2.1 del Decreto 1083 de 2015, sustituido por el artículo 1º del Decreto 1499 de 2017, regula las Políticas de Gestión y Desempeño Institucional, entre las que se encuentran las de *"11. Gobierno Digital, antes Gobierno en Línea" y "12. Seguridad Digital".*

Que el Manual del Sistema Integrado de Gestión del ICBF del 14 de julio de 2022, describe el alcance, las políticas, los objetivos, los procesos, su interacción y la documentación asociada al Sistema Integrado de Gestión frente a las normas y requisitos legales definidos para cada uno de los sistemas que lo conforman.

Que el Instituto Colombiano de Bienestar Familiar - ICBF, mediante Resolución 12068 de 2019, integró y reglamentó el Comité Institucional de Gestión y Desempeño, el cual tiene como propósito orientar la implementación y operación del Modelo Integrado de Planeación y Gestión en la entidad.

Que, de igual manera, la mencionada resolución creó el Subcomité de Arquitectura Empresarial y la Mesa Técnica de Sistemas y Gestión de Información, como instancia asesora de la Entidad, con el fin de promover el análisis integral de los procesos desde diferentes perspectivas, buscando fortalecer de manera articulada, cada uno de los dominios de la Arquitectura Empresarial que permita generar valor a través de las Tecnologías de la Información.

Que el numeral 15 del artículo 3 de la Resolución 12068 de 2019, estableció como responsabilidad del Comité Institucional de Gestión y Desempeño: *"Aprobar y apoyar la implementación de los planes de continuidad del negocio que se establezcan con el fin de mitigar los riesgos asociados a la interrupción de la operación"*, por lo cual resulta necesario adoptar las acciones pertinentes para el efecto, a través del presente acto administrativo.

Que, conforme a los cambios normativos y madurez en el Sistema de Gestión de Seguridad de la Información, es necesaria la revisión y ajuste a la Política de Seguridad de la Información del Instituto y, asimismo, incluir los aspectos relacionados con la Seguridad Digital y la Continuidad de la Operación.

Que en sesión virtual realizada el día 31 de julio de 2023, el Comité Institucional de Gestión y Desempeño aprobó la modificación de la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, ajustada a los cambios y actualizaciones conforme a su operación, decisión que se encuentra contenida en el Acta No 7 de esa fecha.

Que dado lo anterior, se hace necesario adoptar mediante acto administrativo la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación en el ICBF, las Políticas Generales de Manejo, así como definir los lineamientos para su uso y manejo.

Que atendiendo, las actualizaciones y creación de nuevos controles de Seguridad y Privacidad de la Información en la Entidad y con el fin de unificar en un solo acto administrativo, se hace necesario derogar la Resolución 4286 de 2020 "Por la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información, y se deroga la Resolución 9674 de 2018" y la Resolución 5515 de 2021 "Por la cual se modifica el artículo 4 de la Resolución 4286 del 27 de julio de 2020 por la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información, y se deroga la Resolución 9674 de 2018".

En mérito de lo expuesto,

**RESOLUCIÓN No.**

*"Por la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información, y se derogan las Resoluciones 4286 de 2020 y 5515 de 2021"*

## CAPÍTULO I.
## DISPOSICIONES GENERALES.

**ARTÍCULO PRIMERO. Objeto.** Adoptar la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación del Instituto Colombiano de Bienestar Familiar - ICBF, así como las Políticas Generales de Manejo y los lineamientos frente a su uso y manejo de la información.

**ARTÍCULO SEGUNDO. Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación.** El ICBF protege, preserva y administra la integridad, confidencialidad y disponibilidad de la información, así como la seguridad digital y la gestión de la continuidad de la operación, conforme al mapa de procesos, en cumplimiento de los requisitos legales y reglamentarios. La Entidad previene incidentes mediante la gestión de riesgos integrales en seguridad y privacidad de la información, seguridad digital y continuidad del negocio, con la implementación de controles de seguridad físicos y digitales, orientados a la mejora continua en la gestión y el alto desempeño del Sistema de Gestión de Seguridad de la Información, con el fin de prestar servicios con calidad y transparencia a la primera infancia, la niñez, la adolescencia, la juventud y el bienestar de las familias y comunidades colombianas.

**ARTÍCULO TERCERO. Ámbito de Aplicación.** La Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación y las Políticas Generales de Manejo aplican 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, en el desarrollo de la misión institucional y cumplimiento de sus objetivos estratégicos.

**ARTÍCULO CUARTO. Objetivos.** La Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, tendrá los siguientes objetivos:

1. Brindar mecanismos de aseguramiento para el cumplimiento de la confidencialidad, integridad y disponibilidad de la información del ICBF.
2. Mitigar los incidentes de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación en el ICBF.
3. Gestionar los riesgos de seguridad y privacidad de la información, Seguridad Digital y Continuidad de la Operación del ICBF.
4. Establecer los lineamientos necesarios para el manejo de la información y los recursos tecnológicos del ICBF.
5. Fortalecer las capacidades y cultura organizacional de Seguridad de la Información en los colaboradores y contratistas del ICBF.

## CAPÍTULO II.
## POLÍTICAS GENERALES DE MANEJO DE INFORMACIÓN.

**ARTÍCULO QUINTO. Privacidad y Tratamiento de la Información.** Para el tratamiento de la información de los niños, niñas, adolescentes, la juventud, 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 colaboradores y demás partes interesadas 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 que los modifiquen, adicionen o complementen.

**ARTÍCULO SEXTO. Política de Seguridad de los Recursos Humanos.** El ICBF, a través de la Dirección de Información y Tecnología, con el apoyo de la Dirección de Gestión Humana,

propenderá para que los servidores apropien sus responsabilidades frente a la seguridad de la información, con el fin de reducir el riesgo de pérdida, robo, fraude, suplantación de identidad, y/o de los medios tecnológicos de la Entidad, asegurando la confidencialidad, disponibilidad e integridad de la información.

**PARÁGRAFO.** La Dirección de Contratación deberá incluir en las minutas contractuales, cualquiera que sea su modalidad, cláusulas u obligaciones de Seguridad de la Información con el fin de reducir el riesgo de pérdida, robo, fraude, uso indebido, suplantación de identidad de los medios tecnológicos de la Entidad, asegurando la confidencialidad, disponibilidad e integridad de la información.

**ARTÍCULO SÉPTIMO. Política de Gestión de Activos.** El ICBF 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, de acuerdo con la "*Guía para el Desarrollo de Inventario y Clasificación de Activos*."

Con el fin de establecer los controles de seguridad físicos y digitales, las dependencias que tienen la custodia de la información generada en el marco de su función, se encargarán de su protección y de mantener y actualizar el inventario de activos de información relacionados con sus servicios (electrónico, software, físico, hardware, recursos humanos-P, recursos humanos –C, servicio y soporte).

**b. Archivos de Gestión:** La Dirección Administrativa, a través del grupo de gestión documental, deberá implementar los controles necesarios para que los archivos de gestión cuenten con los mecanismos de seguridad, en aras 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 definida 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), tablas de retención documental TRD, el Decreto 1080 de 2015 y lo estipulado en la *Guía para el Desarrollo de Inventario y Clasificación de Activos del ICBF*, regulada por la *Guía de etiquetado y clasificación de la Información*.

**ARTÍCULO OCTAVO. Responsabilidades sobre el uso de los Recursos Tecnológicos.** Todos los colaboradores, proveedores y operadores de servicios tecnológicos que hagan uso de los activos de información del ICBF, tienen la responsabilidad de cumplir las políticas establecidas para su uso apropiado, entendiendo que el uso no adecuado de los recursos pone en riesgo la continuidad de la operación y, por ende, el cumplimento 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 colaboradores y proveedores 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. Está expresamente prohibido enviar o recibir información de carácter personal en el correo institucional, atendiendo que este sólo debe ser usado para fines institucionales. Cada usuario es responsable del contenido del mensaje enviado y de cualquier otra información adjunta al mismo, de acuerdo con la clasificación de la información establecida en 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.
- La Dirección de Información y Tecnología deberá implementar herramientas tecnológicas que prevengan la pérdida o fuga de información de carácter reservada o clasificada, y accesos no autorizados a la infraestructura tecnológica del ICBF.
- Está prohibido el envío de correos masivos a nivel nacional tanto internos como externos, salvo los enviados 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 direcciones regionales está prohibido el envío de correos masivos tanto internos como externos, salvo a través de los Directores Regionales, así como Coordinadores Regionales y de Centro Zonal o quien haga las veces de la Oficina Asesora de Comunicaciones.
- Con el fin de mitigar la suplantación, los directores, subdirectores, jefes de oficina o coordinadores, para apoyar la gestión de su correo electrónico institucional, deberán solicitar a la Mesa de Servicios la delegación del buzón correspondiente, relacionando los funcionarios o contratistas que podrán escribir o responder en nombre de él.
- Todo mensaje sospechoso respecto de su remitente o contenido, deberá ser inmediatamente reportado a la Dirección de Información y Tecnología a través de la Mesa de Servicios, como un posible evento de seguridad, para que sea verificado por los especialistas en cumplimiento del procedimiento establecido.
- Toda persona que tenga asignado correo electrónico institucional, es custodio de sus credenciales de acceso, por lo cual, está expresamente prohibido el uso de su cuenta en páginas o sitios publicitarios, de comercio electrónico, deportivos, agencias matrimoniales, casinos, o cualquier otra ajena a los fines de la Entidad, siendo su responsabilidad en caso de que este sea vulnerado, asumiendo las consecuencias legales y disciplinarias a que haya lugar.
- Está expresamente prohibido el uso del correo institucional para la divulgación y envío de anónimos y 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 entidades o ciudadanos, sin la debida autorización de la Directora General, Directores Regionales, Subdirector General, Directores Misionales y/o Director de Planeación y Control de Gestión, previa revisión de la Oficina Asesora de Comunicaciones y de la Dirección de Planeación y Control de Gestión, en caso de cifras oficiales.
- La Dirección de Información y Tecnología deberá implementar un control de cifrado para los mensajes de correo electrónico institucional.
- El correo electrónico institucional en sus mensajes deberá contener una sentencia de confidencialidad, que será diseñada por la Dirección de Información y Tecnología a través de la Subdirección de Recursos Tecnológicos, la cual se reflejará 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 de control interno, Oficina Asesora de Comunicaciones y la Dirección de Planeación y Control de Gestión.
- Está expresamente prohibido distribuir, copiar, reenviar información del ICBF a través de correos personales o sitios web diferentes a los autorizados en el marco de sus funciones u obligaciones contractuales.
- 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 ICBF se reserva el derecho de monitorear los accesos y el uso de los buzones de correo institucionales de todos sus colaboradores, proveedores y operadores, además podrá realizar copias de seguridad en cualquier momento, sin previo aviso, así como limitar el acceso temporal o definitivo, por solicitud expresa del nominador, ordenador del gasto, supervisor del contrato, jefe inmediato, Directora General, Jefe de Oficina de Control Interno Disciplinario o Director de Gestión

Humana a la Dirección de Información y Tecnología, así como a todos los servicios y accesos a sistemas de información de la Entidad o de terceros operados en la Entidad.

- La Subdirección de Recursos Tecnológicos deberá configurar el método de autenticación multifactor a los usuarios de los colaboradores al momento de iniciar la sesión para acceder a las cuentas y servicios ligadas al dominio de ICBF, con el cual se validará la identidad y se implementará el acceso seguro.

**b. Del Uso de Internet:** La Dirección de Información y Tecnología establece controles en la Guía de Políticas de Navegación, basados en categorías, las cuales deben ser implementadas por la Subdirección de Recursos Tecnológicos. Asimismo, será responsabilidad de los colaboradores cumplir a cabalidad con las directrices y políticas de seguridad y privacidad de la información, así:

- El servicio de Internet es de uso exclusivo, para propósitos laborales, contractuales e institucionales. La navegación en Internet debe realizarse de forma razonable y con propósitos laborales.
- Los servicios a los que un determinado usuario pueda acceder en internet dependerán de la categoría que se le asigne, la cual se establece a partir de la dependencia a la que pertenezca, obligaciones contractuales, funciones o roles que desempeña en el ICBF y para las cuales esté formal y expresamente autorizado.
- Está expresamente prohibido el envío, descarga y 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 descarga de cualquier tipo de software o archivos de fuentes externas, y 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 colaboradores, además de limitar el acceso a determinadas páginas de Internet, 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, obligaciones y responsabilidades de colaboradores. Por ello, su uso está sujeto a las siguientes directrices:

- Los elementos tecnológicos se emplearán de manera exclusiva y bajo la completa responsabilidad de los colaboradores, a quienes se le haya asignado, 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 por la Dirección de Información y Tecnología
- 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 y que no fueron desarrollados por la Entidad, deberán ser reportadas a la Dirección de Información y Tecnología a través de la Subdirección de Sistemas Integrados de Información, con el soporte de cesión de derechos patrimoniales, para que ella a su vez verifique si cumple con los lineamientos y requerimientos establecidos, dentro de la política de desarrollo seguro.
- En caso de que el colaborador deba hacer uso de equipos personales, estos deberán cumplir con las reglas de seguridad y lineamientos establecidos en la Guía para uso de dispositivos personales BYOD y solo podrá conectarse a la red del ICBF, una vez esté sea avalado por los ingenieros de la Subdirección de Recursos Tecnológicos, Ingenieros Regionales o soporte en sitio. La Subdirección de Recursos Tecnológicos deberá realizar la revisión de los requisitos antes mencionados, de manera periódica, en los equipos autorizados para conectarse a la red de ICBF. El colaborador será responsable de custodiar la información institucional en cuanto a su almacenamiento, y esta no debe reposar en el disco local del equipo personal sino en el espacio asignado en OneDrive o SharePoint.
- Es responsabilidad de los funcionarios y contratistas guardar y almacenar su información institucional en OneDrive y SharePoint, con el fin de custodiar su información propendiendo por su

protección y disponibilidad durante el tiempo de su vinculación laboral o contractual, y al finalizar esta con la Entidad.

- Las copias de seguridad de la información de los colaboradores deberán ser solicitadas únicamente por el jefe inmediato o quien haga las veces de supervisor del contrato y deberá tramitarse a través de la Mesa de Servicio o por requerimiento de las autoridades competentes.
- Está expresamente prohibido almacenar información personal en los equipos de propiedad de ICBF o en cualquier otro repositorio institucional.
- Los usuarios no deben mantener o almacenar en las herramientas, equipos e infraestructura tecnológica información personal, archivos de video, música y fotos que no sean de carácter institucional o que atenten con los derechos de autor o propiedad intelectual de los mismos.
- No está permitido fumar, ingerir alimentos o bebidas en el área de trabajo donde se encuentren elementos tecnológicos, archivos de gestión o información física que pueda ocasionar un incidente de seguridad de la información
- Cuando un colaborador, proveedor u operador cese sus funciones o culmine la ejecución del contrato con el ICBF, conforme con la solicitud realizada por el G58 de la dependencia a la Mesa de Soluciones, todos los privilegios sobre los recursos informáticos otorgados le serán suspendidos inmediatamente; el supervisor o jefe inmediato velará porque la información de estos se almacene en el repositorio de almacenamiento en nube definido por el ICBF.
- Es responsabilidad del jefe inmediato o supervisor del contrato solicitar a través del G58 la inactivación de la cuenta, así como de los aplicativos o sistemas de información que maneje, cuando un colaborador presente novedades administrativas (vacaciones, permisos, incapacidades médicas, calamidad doméstica terminación del contrato u otro que supere los 8 días), con el fin de evitar posibles incidentes de seguridad de la información.
- Cuando un funcionario, colaborador, proveedor u operador se le termina su vínculo administrativo o finaliza el contrato, el supervisor o jefe inmediato es el encargado de la custodia de los recursos de información, incluyendo los derechos de propiedad intelectual de acuerdo con la normativa vigente.
- Todos los colaboradores, proveedores y operadores deben dar estricto cumplimiento a 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.
- No está permitido el uso de botellones de agua cerca a elementos tecnológicos o archivos de gestión, lo anterior para evitar un incidente de seguridad de la información.
- No está permitido realizar conexiones o derivaciones eléctricas que pongan en riesgo los elementos tecnológicos por fallas en el suministro eléctrico a los equipos de cómputo, salvo en aquellos casos que sean autorizados por la Dirección Administrativa o quien haga sus veces en el nivel Regional o Zonal.
- Las únicas personas autorizadas para hacer modificaciones o actualizaciones en los equipos de cómputo, impresoras, escáner, switches, servidores y demás 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 desempeñar esta labor.
- El uso de medios removibles solamente será justificado y autorizado a los colaboradores del ICBF con el aval del supervisor del contrato o jefe inmediato, exceptuando situaciones donde la Entidad no esté en capacidad de proveer medios de almacenamiento en nube como OneDrive o SharePoint o cuando sus actividades o funciones sean desempeñadas en zonas rurales dispersas, donde la Entidad no tiene los medios para proveer acceso a las herramientas tecnológicas antes mencionadas o cuando sea necesario para cumplir con los objetivos en el relacionamiento con usuarios externos. Por lo anterior se requiere que en el momento que se habilite un puerto, el dueño de proceso identifique y trate el riesgo de seguridad de la información relacionado con fuga y pérdida de información e infección por Malware.
- La única dependencia autorizada para trasladar los elementos y recursos tecnológicos de un puesto a otro será la Dirección de Información y Tecnología o quien haga sus veces en el nivel regional y zonal; sin embargo, para los traslados desde y hacia el almacén, será la Dirección Administrativa, o el Grupo Administrativo o Grupo de Gestión de Soporte en el caso de las Regionales. Lo anterior, con el fin de llevar el control de inventarios. En tal virtud, toda reasignación de equipos deberá ajustarse a los procedimientos para la gestión de bienes de la Entidad.
- La pérdida o daño de elementos o recursos tecnológicos, o de alguno de sus componentes, deberá ser informada de inmediato a la Dirección Administrativa y al superior inmediato o supervisor, por

el funcionario o contratista a quien se le hubiere asignado, allegando la respectiva denuncia en caso de pérdida o robo ante la autoridad competente.

- La pérdida de información física o digital que comprometa la disponibilidad, confidencialidad e integridad, deberá 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 física o digital deberá ser reportado a través de la Mesa de Servicios, siguiendo el procedimiento establecido.
- La Dirección de Información y Tecnología es la única dependencia autorizada para la administración del software, el cual no deberá ser copiado, suministrado a terceros ni utilizado para fines personales, en cumplimiento a los derechos de autor
- Se prohíbe la conexión de módems o cualquier otro mecanismo de conexión, sin la correspondiente autorización de la Dirección de Información y Tecnología.
- 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.
- La conexión a la red wifi institucional para funcionarios deberá ser administrada desde la Dirección de Información y Tecnología mediante un SSID (Service Set Identifier) único a nivel nacional.
- No se podrá conectar dispositivos celulares personales a la red wifi de funcionarios, salvo los de la Oficina Asesora de Comunicaciones, Dirección General y los aprobados por la Dirección de Información y Tecnología, o quien haga sus veces, en las sedes Regionales y Zonales, a través de una solicitud por módulo de autoservicio en la herramienta de Mesa de Servicios.
- Está prohibido el uso de herramientas o páginas de mensajería instantánea distintas a las autorizadas por la Entidad como el envío de documentos etiquetados como clasificada, reservada, fotografías, audios y videos con información sensible, salvo los usuarios que tengan permiso conforme a la Guía de Políticas de Navegación.
- Todo dispositivo móvil personal que requiera acceder a los servicios tecnológicos de la Entidad deberá cumplir con la política y lineamientos definidos en la Guía para el uso de dispositivos personales.

**d. Del Uso de los Sistemas o Herramientas de Información:** Todos los colaboradores, proveedores y operadores 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 Contraseña) son de carácter estrictamente personal e intransferible; los colaboradores, proveedores y operadores no deben revelarlas a terceros ni utilizar contraseñas ajenas.
- Todo colaborador es responsable del cambio de contraseña de acceso a los sistemas de información o recursos informáticos periódicamente.
- Todo colaborador es responsable de los registros y modificaciones de información que se hagan a nombre de su cuenta de usuario.

**ARTÍCULO NOVENO. Política de Control de Acceso.** Los propietarios de los activos de información deberán 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.

**PARÁGRAFO 1.** El área funcional será la encargada de brindar lineamientos y dar cumplimiento a las políticas establecidas en el control de acceso a los usuarios de los servicios asignados en los sistemas de información, que se encuentran bajo su administración.

**PARÁGRAFO 2.** La Subdirección de Recursos Tecnológicos en conjunto con la Subdirección de Sistemas Integrados de Información, establecerá las configuraciones de las políticas en los sistemas de información y comunicaciones para el control de acceso a los activos de información.

**PARÁGRAFO 3.** Solo los usuarios autorizados por la Dirección de Información y Tecnología podrán instalar software y/o hardware en los equipos, servidores e infraestructura de telecomunicaciones, así como el uso de herramientas que permitan realizar tareas de mantenimiento, revisión de software, restauración de copias de seguridad cuando se requiera y eliminar software malicioso.

**PARÁGRAFO 4.** La conexión remota VPN a la red del ICBF, debe ser justificada y solicitada por los Directores o Jefes de Oficina a través de la Mesa Informática de Soluciones y es la Dirección de Información y Tecnología en cabeza de la Subdirección de Recursos Tecnológicos quién validará la solicitud.

**ARTÍCULO DÉCIMO. Política de Criptografía.** La Dirección de Información y Tecnología brindará de acuerdo con los requerimientos del ICBF, herramientas que permitan el cifrado de la información para proteger la confidencialidad, integridad y disponibilidad de la información clasificada o reservada, en sistemas de información, correo electrónico y mecanismos de transferencia de información interna o externa.

**ARTÍCULO DÉCIMO PRIMERO. Política de Seguridad Física y del Entorno.** El ICBF contará 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 seguras (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 evitar afectación a la confidencialidad, disponibilidad e integridad de la información de la Entidad.

**PARÁGRAFO 1.** Todos los colaboradores y visitantes que se encuentren en las instalaciones físicas del ICBF deben estar debidamente identificados, con un documento, el cual deberá portarse en un lugar visible.

**PARÁGRAFO 2.** Los visitantes del ICBF siempre deberán permanecer acompañados por un colaborador debidamente identificado.

**PARÁGRAFO 3.** El personal de empresas contratistas que desempeñen funciones de forma permanente en las instalaciones del ICBF, deberá estar identificado con carné, o chalecos o algún distintivo que lo identifique como contratista de un operador. También deberá portar el carné de la ARL.

**PARÁGRAFO 4.** El ICBF a través de la Dirección Administrativa realizará la contratación de un proveedor quien tendrá a cargo las bitácoras de ingreso/salida, sistemas de control de acceso implementados, así como los sistemas de video seguridad (Circuito cerrado de televisión CCTV), para realizar el monitoreo de seguridad en las instalaciones.

**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 la plataforma tecnológica que soporta la operación del ICBF. Asimismo, velará por la eficiencia de los controles asociados a los recursos tecnológicos protegiendo la confidencialidad, integridad y disponibilidad de la información, asegurando que los cambios efectuados sobre estos se realicen de manera controlada y cuenten con la autorización respectiva. De igual manera, deberá proveer la capacidad de procesamiento requerida en los recursos tecnológicos y los sistemas de información del ICBF, efectuando proyecciones de crecimiento y provisiones en la plataforma tecnológica de acuerdo con las necesidades de la Entidad.

**PARÁGRAFO 1.** La Dirección de Información y Tecnología, a través de la Subdirección de Recursos Tecnológicos, deberá realizar y mantener copias de seguridad de la información de la Entidad, 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.

**PARÁGRAFO 2.** La respectiva copia de seguridad se realizará de acuerdo con el esquema definido previamente en el documento Procedimiento Gestión Copias de Seguridad de la Entidad, el cual contiene los lineamientos establecidos 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. Asimismo, dispondrá y monitoreará los mecanismos necesarios de seguridad para proteger la integridad y la confidencialidad de la información del ICBF.

**PARÁGRAFO 1.** Como parte de sus términos y condiciones iniciales de trabajo, los colaboradores, cualquiera que sea su nivel jerárquico dentro de la Entidad, firmarán un Formato de Compromiso de Confidencialidad de información, dando cumplimiento a lo que respecta al tratamiento de la información de la Entidad y, de igual manera, el formato Autorización de tratamiento de datos personales, 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. Asimismo, mediante el Compromiso de Confidencialidad el colaborador declarará conocer y aceptar la existencia de determinadas actividades que pueden ser objeto de control y monitoreo, las cuales deben ser detalladas con el fin de no violar el derecho a la privacidad ni sus derechos. La gestión de la suscripción del compromiso de confidencialidad por parte de los colaboradores será responsabilidad del jefe directo o supervisor de contrato.

**PARÁGRAFO 2.** Para el caso del personal que ejecute tareas propias del ICBF y haya sido contratado en el marco de un contrato o convenio con el ICBF, en la carpeta de ejecución del contrato deberá reposar un compromiso de confidencialidad debidamente suscrito por el Representante Legal de la empresa contratista o con la cual se realiza el convenio.

**PARÁGRAFO 3.** La Dirección de Información y Tecnología deberá segmentar la red, de modo que permita separar los grupos de servicios de información.

**PARÁGRAFO 4.** El Oficial de Datos Personales adscrito a la Dirección de Planeación, establecerá los mecanismos y lineamientos para el intercambio de información con las entidades externas o internas.

**PARÁGRAFO 5.** Los colaboradores deberán emplear los puntos de red habilitados para la conexión de equipos institucionales o personales debidamente autorizados.

**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.

**PARÁGRAFO 1.** 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.

**PARÁGRAFO 2.** Cualquier software que opere en el Instituto y no haya sido reportado a la Dirección de Información y Tecnología conforme a los lineamientos establecidos, no será

responsabilidad de esta dependencia, no se le brindará soporte y no se le salvaguardará la información.

**PARÁGRAFO 3.** La Dirección de Información y Tecnología deberá propender porque los sistemas de información o aplicativos incluyan controles de seguridad y cumplan con las políticas de seguridad de la información.

**PARÁGRAFO 4.** La Dirección de información y Tecnología en conjunto con la Subdirección de Sistemas de Información deberá realizar pruebas de funcionamiento y de seguridad a los nuevos sistemas, actualizaciones y/o aplicaciones en ambiente de pruebas, para validar la necesidad y operatividad de estos, previo a la aprobación e implementación.

**PARÁGRAFO 5.** La Subdirección de Sistemas Integrados de Información desarrollará y/o adquirirá el software requerido para los procesos de la Sede de la Dirección General, de manera coordinada con el Área que manifieste la necesidad del software y se establecerán claramente los requerimientos funcionales, operacionales y especificaciones técnicas para la adquisición o desarrollo de sistemas de información y/o comunicaciones, contemplando requerimientos y requisitos de seguridad de la información.

**PARÁGRAFO 6.** Los desarrollos de la Entidad deberán estar completamente documentados, de acuerdo con el manual de procedimiento vigente, igualmente todas las versiones de los desarrollos se deberán preservar adecuadamente.

**PARÁGRAFO 7.** La Subdirección de Sistemas Integrados de Información deberá desarrollar estrategias para analizar la seguridad en los sistemas de información.

**PARÁGRAFO 8.** Todo nuevo hardware y software que se vaya a adquirir y conectar en la Entidad, por cualquier dependencia o proceso, deberá ser revisado y aprobado por la Dirección de Información y Tecnología, en cabeza de la Subdirección de Recursos Tecnológicos y la Subdirección de Sistemas Integrados de Información, para su correcto funcionamiento y protección de la información.

**PARÁGRAFO 9.** La Dirección de Información y Tecnología implementará reglas y herramientas que restrinjan la instalación de software no autorizado o que no esté aprobada en la línea base de los activos de información del ICBF.

**PARÁGRAFO 10.** El software que se adquiera a través de proyectos, programas o convenios, deberá establecer los lineamientos para la supervisión y seguimiento a las actividades de desarrollo contratado, los cuales deben quedar inmersos en las cláusulas y/o especificaciones técnicas.

**PARÁGRAFO 11.** El área funcional deberá solicitar y /o autorizar la baja de cualquier software y con base en ello, la Dirección de información y Tecnología a través de la Subdirección de Recursos Tecnológicos y la Subdirección de Sistemas Integrados de Información, realizará las acciones pertinentes.

**PARÁGRAFO 12.** La Subdirección de Sistemas Integrados de Información, deberá implementar métodos y/o técnicas para el desarrollo de software seguro, estas deben incluir definiciones y requerimientos de seguridad, buenas prácticas para desarrollo de software seguro, que le permita a los desarrolladores aplicarlas de manera clara, eficiente y con calidad. Cuando el desarrollo provenga de un área diferente estos deben garantizar el cumplimiento de los lineamientos de la Subdirección de Sistemas Integrados de 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 y revisión del cumplimiento de las políticas, procedimientos y cláusulas contractuales de seguridad de la información, conforme a lo establecido en la Guía de Adquisición de Bienes y Servicios con Calidad.

**PARÁGRAFO 1.** Los operadores deberán aceptar y firmar el acuerdo de confidencialidad establecido por el ICBF.

**PARÁGRAFO 2.** Los supervisores de contratos deberán realizar seguimiento, control y revisión de los servicios suministrados por los proveedores y/o contratistas.

**PARÁGRAFO 3.** Los supervisores de contrato deberán establecer mecanismos o condiciones con los contratistas o proveedores de servicios tecnológicos, que permitan garantizar el cumplimiento del procedimiento de gestión de cambios en los servicios suministrados a la Entidad.

**PARÁGRAFO 4**. Los proveedores u operadores deberán informar y gestionar ante el supervisor del contrato, las activaciones y desactivaciones de usuarios que se deban realizar de su personal a cargo por novedades administrativas (vacaciones, permisos, incapacidades médicas, calamidad doméstica terminación del contrato u otro que supere los 8 días), con el fin de evitar posibles incidentes de seguridad de la información.

**ARTÍCULO DÉCIMO SEXTO. Política de Gestión de Incidentes de Seguridad de la Información.** El ICBF promoverá entre los colaboradores, proveedores y operadores el reporte de incidentes relacionados con la seguridad de la información y sus medios, reporte y seguimiento. Asimismo, 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. La Dirección General o quien ésta delegue, será la única autorizada para reportar incidentes de seguridad ante las autoridades, así como, hacer pronunciamientos oficiales ante entidades externas, medios de comunicación o la ciudadanía.

**PARÁGRAFO.** De acuerdo con la criticidad del incidente, la Dirección de Información y Tecnología lo reportará al Equipo de respuesta a incidentes de seguridad informática, siguiendo los lineamientos y parámetros que este defina.

**ARTÍCULO DÉCIMO SÉPTIMO. Política de la Continuidad de la Operación.** El ICBF dispondrá los planes necesarios para la implementación del proceso de continuidad de la Operación Tecnológica. La Secretaría General liderará la elaboración del Análisis de Impacto al Negocio (BIA) y del Plan de Continuidad de la Operación, así como la activación de este, cuando sea necesario.

**PARÁGRAFO 1.** La Secretaría General con apoyo de la Dirección de Información y Tecnología deberá generar un Plan de Continuidad de la Operación, documentando e implementando procesos y procedimientos, para asegurar la continuidad requerida por la Entidad.

**PARÁGRAFO 2.** El Plan de Continuidad de la Operación Tecnológica deberá incluirse en el Plan de Continuidad de la Operación del ICBF. Los Planes de Contingencia serán activados conforme a la operación, así como cualquier estrategia alineada a la Continuidad de la Operación dentro de la prestación del servicio del Instituto Colombiano de Bienestar Familiar.

**PARÁGRAFO 3.** La Dirección de Información y Tecnología elaborará el Plan de Recuperación de Desastres, el cual deberá incluir como mínimo los procedimientos, requisitos de seguridad de la información, recuperación y retorno a la normalidad.

**RESOLUCIÓN No.**

*"Por la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información, y se derogan las Resoluciones 4286 de 2020 y 5515 de 2021"*

**ARTÍCULO DÉCIMO OCTAVO. Política de Cumplimiento.** El ICBF velará por la identificación, documentación, seguimiento 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, Ley de transparencia y del derecho de acceso a la información pública nacional y las consignadas en la Matriz de Requisitos Legales del ICBF.

**ARTÍCULO DÉCIMO NOVENO. Lineamientos de las Políticas de Seguridad de la Información.** Todas las políticas contenidas en el Capítulo II de este acto administrativo se encuentran reglamentadas en los documentos, Declaración de Aplicabilidad y Manual de Política de Seguridad de la Información, los cuales están anexos al Manual del Sistema Integrado de Gestión del ICBF y son parte integral de este documento.

## CAPÍTULO III.
## REVISIÓN, VIGENCIA Y DEROGATORIA.

**ARTÍCULO VIGÉSIMO. Revisión.** La Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, 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 revisado por el Comité Institucional de Gestión y Desempeño.

**ARTÍCULO VIGÉSIMO PRIMERO. Vigencia y Derogatoria.** La presente Resolución rige a partir de la fecha de su publicación, deroga la Resolución No. 4286 del 2020 y la Resolución No. 5515 de 2021, así como todas aquellas disposiciones que le sean contrarias.

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

**ASTRID ELIANA CACERES CARDENAS**
Directora General

**Aprobó:** Jose Ebert Bonilla Olaya___ Director de Información y Tecnología / Milton Fabian Forero Melo___ Director de Planeación y Control de Gestión / Daniel Eduardo Lozano Bocanegra ___Jefe Oficina Asesora Jurídica

**Revisó:** Ginna Paola Garcia Bohorquez___ Contratista Dirección de Información y Tecnología
**Proyectó**: Astrid Vannessa Castro Cortes___ Contratista Dirección de Información y Tecnología / Teresa Quilindo Sarasti___ Contratista Dirección de Información y Tecnología