RESOLUCIÓN No. 3248 del 2 de Julio de 2025

"Por la cual se adopta la Política de Seguridad y Privacidad de la Información, Ciberseguridad 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 414 de 2024"

LA DIRECTORA GENERAL DEL INSTITUTO COLOMBIANO DE BIENESTAR FAMILIAR (ICBF) "CECILIA DE LA FUENTE DE LLERAS"

En uso de sus facultades legales y estatutarias y, en especial de las que confieren la Ley 7 de 1979, el artículo 4 de la Ley 87 de 1993, el artículo 78 de la Ley 489 de 1998, y el artículo 2.2.2.2.1 del Decreto 1083 de 2015 y,

CONSIDERANDO:

Que el artículo 209 de la Constitución Política señala que *"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 el artículo 2.2.9.1.1.3 del Decreto 1078 de 2015, establece los principios de la Política de Gobierno Digital, dentro de los que se encuentra el principio de seguridad de la información, el cual *"busca 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".* De igual manera, el artículo 2.2.9.1.2.1 establece que la estructura de los elementos de la Política de Gobierno Digital se desarrollará a través de un esquema que articula sus componentes, a saber: gobernanza, innovación pública digital, habilitadores, líneas de acción, e iniciativas dinamizadoras con el fin de lograr su objetivo.

Que el Decreto 1499 de 2017, que modificó el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector de Función Pública, adoptó el Modelo Integrado de Planeación y Gestión (MIPG), definiéndolo en su artículo 2.2.22.3.2 como el *"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".*

Que el artículo 2.2.22.2.1 del Decreto 1083 de 2015 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 mediante la Resolución 8650 de 2021 el ICBF integró y reglamentó el Comité Institucional de Gestión y Desempeño, cuyo objeto es orientar la implementación y operación del Modelo Integrado de Planeación y Gestión en la Entidad. A su vez, en el numeral 15 del artículo 3, señaló que corresponde a esta instancia *"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",* razón por la cual, es necesario adelantar las acciones pertinentes para el efecto.

El Documento CONPES 3854 de 2016, establece la Política Nacional de Seguridad Digital en la República de Colombia, fortaleciendo las capacidades de las múltiples partes interesadas, para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital y se generarán mecanismos permanentes para impulsar la cooperación, colaboración y asistencia en materia de seguridad digital, a nivel nacional e internacional, con un enfoque estratégico.

El Documento CONPES 3995 de 2020 formula la Política Nacional de Confianza y Seguridad Digital en la República de Colombia, estableciendo medidas para ampliar la confianza digital y mejorar la seguridad digital de manera que Colombia sea una sociedad incluyente y competitiva en el futuro digital, fortaleciendo las capacidades en seguridad digital de los ciudadanos, del sector público y del sector privado del país; actualizando el marco de gobernanza en materia de seguridad digital para aumentar su grado de desarrollo y finalmente, se analizará la

adopción de modelos, estándares y marcos de trabajo en materia de seguridad digital, con énfasis en nuevas tecnologías.

Que, de acuerdo con los cambios normativos y madurez del Sistema de Gestión de Seguridad de la Información, se adelantó la revisión y ajuste a la Política de Seguridad de la Información del Instituto Colombiano de Bienestar Familiar (ICBF), en el sentido de incluir los aspectos relacionados con la ciberseguridad y la continuidad de la operación.

Que la Resolución 500 de 2021 del Ministerio de Tecnologías de la Información y las Comunicaciones, establece lineamientos generales para la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI), la guía de gestión de riesgos de seguridad de la información y el procedimiento para la gestión de los incidentes de seguridad digital, y, establece los lineamientos y estándares para la estrategia de seguridad digital, a los sujetos obligados señalados en el artículo 2.2.9.1.1.2. del Decreto 1078 de 2015.

El artículo 5 de la misma Resolución, establece que los sujetos obligados deben adoptar la estrategia de seguridad digital en la que se integren los principios, políticas, procedimientos, guías, manuales, formatos y lineamientos para la gestión de la seguridad de la información digital. Dicha estrategia se debe incluir en el Plan de Seguridad y Privacidad de la Información que se integra al Plan de Acción en los términos artículo 2.2.22.3.14. del capítulo 3 del Título 22 de la Parte 2 del Libro 2 del Decreto 1083 de 2015, Único Reglamentario del Sector de Función Pública, o la norma que la modifique, adicione, subrogue o derogue. Así como, adoptar el Modelo de Seguridad y Privacidad de la Información (MSPI) señalado en el Anexo 1 de la misma resolución, como habilitador de la política de Gobierno Digital.

Que de conformidad con los Planes Institucionales Estratégicos aprobados por el Comité Institucional de Gestión y Desempeño en sesión del 29 de enero de 2025 y la transición de la norma ISO 27001:2022, se hace necesario alinear la Política de Seguridad y Privacidad de la Información, Ciberseguridad y Continuidad de la Operación del Instituto Colombiano de Bienestar Familiar (ICBF).

Que la Resolución 414 del 14 de febrero de 2024 adoptó la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación del Instituto Colombiano de Bienestar Familiar (ICBF), las Políticas Generales de manejo y se definen lineamientos frente al uso y manejo de la información.

Que en virtud de lo establecido en el numeral 14 del artículo 3 de la Resolución 8650 de 2021, en sesión del 24 de mayo 2024 el Comité Institucional de Gestión y Desempeño aprobó la modificación de la Política General de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de Operación.

Que en cumplimiento del trámite establecido en el parágrafo 3 de artículo 6 de la Resolución 0353 del 7 de febrero de 2023 del ICBF, se surtió la publicación correspondiente al proyecto de acto administrativo en la página web de la Entidad, del 14 al 24 de marzo al 2025, sin que hubiesen recibido observaciones, sugerencias o comentarios, emitiéndose por parte de la Dirección de Servicios y Atención del ICBF la respectiva certificación el día 27 de marzo del 2025.

Que dado lo anterior, y en el marco del Sistema de Gestión de Seguridad de la Información (SGSI) del ICBF, se hace necesario adoptar la Política de Seguridad y Privacidad de la Información, Ciberseguridad y Continuidad de la Operación en el ICBF, las Políticas Generales de Manejo, así como definir los lineamientos para su uso y manejo y, como consecuencia, derogar la Resolución 414 del 14 de febrero de 2024.

En mérito de lo expuesto,

RESOLUCIÓN No. 3248 del 2 de Julio de 2025

"Por la cual se adopta la Política de Seguridad y Privacidad de la Información, Ciberseguridad 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 414 de 2024"

RESUELVE:

CAPÍTULO I. DISPOSICIONES GENERALES

ARTÍCULO 1. Objeto. Adoptar la Política de Seguridad y Privacidad de la Información, Ciberseguridad 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 2. Política de Seguridad y Privacidad de la Información, Ciberseguridad y Continuidad de la Operación. El ICBF protege, preserva y administra la integridad, confidencialidad, disponibilidad de la información, así como la ciberseguridad y la gestión de la continuidad de la operación, conforme al mapa de procesos y en cumplimiento de los requisitos legales y reglamentarios. Así mismo, la entidad previene incidentes mediante la gestión de riesgos integrales en seguridad y privacidad de la información, ciberseguridad 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, partiendo de las necesidades y expectativas de las partes interesadas (stakeholders), promoviendo por la protección integral de los derechos de los niños, niñas, adolescentes, familias y colaboradores del ICBF.

ARTÍCULO 3. Ámbito de aplicación. La Política de Seguridad y Privacidad de la Información, Ciberseguridad y Continuidad de la Operación, así como las Políticas Generales de Manejo, se aplican en todos los lugares donde el Instituto Colombiano de Bienestar Familiar (ICBF) tenga presencia o realice actividades. Esto incluye la recolección, procesamiento, almacenamiento, recuperación, intercambio y consulta de información, asegurando el cumplimiento de la misión institucional y los objetivos estratégicos.

ARTÍCULO 4. Objetivos. La Política de Seguridad y Privacidad de la Información, Ciberseguridad y Continuidad de la Operación, tendrá los siguientes objetivos:

1. Desarrollar e implementar mecanismos de aseguramiento para garantizar la protección de la confidencialidad, integridad y disponibilidad de la información de la entidad, utilizando controles robustos.
2. Mitigar los incidentes relacionados con la seguridad y privacidad de la información, así como con la ciberseguridad, mediante el cumplimiento del procedimiento de gestión de incidentes y la implementación de controles preventivos y correctivos y la adopción de medidas de respuesta de manera efectiva, eficaz y eficiente.
3. Gestionar los riesgos relacionados con la seguridad y privacidad de la información, ciberseguridad y continuidad de la operación, de acuerdo con los requisitos de la norma ISO 27001:2022, a través de la identificación, evaluación y tratamiento de riesgos, así como la implementación de controles adecuados para mitigar posibles amenazas y asegurar la resiliencia operativa de establecer los lineamientos necesarios para el manejo de la información y los recursos tecnológicos del ICBF.
4. Fortalecer las capacidades de cambio y cultura en seguridad de la información entre las partes interesadas (stakeholders), mediante estrategias de capacitación, socializaicón, concienciación y la implementación de mejores prácticas en ciberseguridad y privacidad de la información.
5. Establecer lineamientos necesarios para el manejo de la información y los recursos tecnológicos del ICBF.
6. Cumplir con los requisitos legales, reglamentarios y regulatorios, así como con las normas técnicas colombianas en materia de seguridad y privacidad de la información, ciberseguridad y continuidad de la operación. Esto incluye la implementación de políticas y procedimientos que aseguren la conformidad con las leyes y estándares aplicables, garantizando la protección de la información y la resiliencia operativa de la entidad.

CAPÍTULO II.
CONTROLES ORGANIZACIONALES

ARTÍCULO 5. Privacidad y tratamiento de la información. Para proteger la confidencialidad, disponibilidad e integridad en el tratamiento de la información de los niños, niñas, adolescentes y familias 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 (stakeholders), que participan en el desarrollo de las funciones de dicho mandato, el ICBF cuenta con la *"Política de Privacidad y 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.

PARÁGRAFO 1. Todos los colaboradores, proveedores y terceros que tengan acceso a la información personal gestionada por la entidad deben proteger la privacidad y la seguridad de dicha información. Esto implica cumplir con las leyes, normas y regulaciones aplicables, y actuar conforme a los principios de transparencia, consentimiento y seguridad.

PARÁGRAFO 2. La Dirección de Información y Tecnología implementará controles para limitar el acceso a la información personal solo a aquellos servidores públicos y contratistas que necesiten dicha información para cumplir con sus obligaciones contractuales o actividades laborales.

ARTÍCULO 6. Política de gestión de activos. El ICBF, a través de la Dirección de Información y Tecnología, establecerá las directrices para la identificación, clasificación, etiquetado y uso adecuado de los activos de información. El objetivo es garantizar su protección, siguiendo las siguientes directrices:

a. **Identificación de activos:** catalogar todos los activos de información en los procesos de la Sede de la Dirección General y Regionales. Mediante esta actividad se realiza la identificación inicial de un activo como requisito para efectuar la valoración del riesgo.

b. **Clasificación de activos:** asignar niveles de criticidad a cada activo. La clasificación tiene como objetivo asegurar que la información tenga el nivel de protección adecuado conforme a su criticidad. La información debe clasificarse en términos de confidencialidad, disponibilidad, integridad para el ICBF.

c. **Etiquetado de activos:** identificar su nivel de criticidad de la información PÚBLICA, CLASIFICADA Y RESERVADA. Seleccionar la clasificación que contiene el activo de información de acuerdo con las Leyes 1712 de 2014, 1581 de 2012, el Grupo 5 de controles organizacionales, anexo A de la norma ISO 27001:2022, la normatividad interna aplicable del ICBF o las tablas de retención documental.

d. **Uso adecuado:** definir y comunicar las políticas de uso correcto de los activos. 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.

e. **Protección de activos:** implementar medidas de seguridad para proteger la confidencialidad, integridad y disponibilidad de la información.

f. **Inventario de activos:** los activos deben ser identificados, clasificados y controlados

para garantizar su uso adecuado, protección y recuperación ante desastres. Por ello, es necesario mantener un inventario detallado de los activos de información de propiedad del ICBF, discriminado por procesos. Esto asegura una gestión eficiente y una respuesta rápida en caso de incidentes, de acuerdo con la *"Guía para el Desarrollo de Inventario y Clasificación de Activos".*

Con el fin de establecer controles de seguridad físicos y digitales, las dependencias responsables de la custodia de la información generada en el marco de sus funciones deberán encargarse de su protección. Además, deberán mantener actualizado el inventario de activos de información.

ARTÍCULO 7. Política de control de acceso. Los propietarios de los activos de información, considerando el tipo de activo y su criticidad, deberán cumplir con los controles y buenas prácticas establecidas por la Dirección de Información y Tecnología. Estas incluyen medidas de control de acceso a nivel de red, sistema operativo, sistemas de información, servicios de tecnologías de la información (on premise o en nube) e infraestructura física. El propósito es mitigar los riesgos asociados al acceso no autorizado a la información y los servicios tecnológicos, salvaguardando la integridad, disponibilidad y confidencialidad de los datos.

PARÁGRAFO 1. La Dirección de Información y Tecnología, en cabeza de la Subdirección de Recursos Tecnológicos, será la encargada de administrar y proteger las identidades digitales de los colaboradores, operadores y terceros, asegurando que solo las personas autorizadas tengan acceso a los recursos adecuados con el fin de proteger los datos sensibles o datos personales mediante el control de acceso para garantizar la integridad y confidencialidad de la información.

Para realizar la Gestión y protección de Identidades el ICBF cuenta con:

- **Autenticación:** se implementará el doble factor de autenticación con el objeto de verificar la identidad de colaboradores, operadores y terceros antes de permitir el acceso a los recursos tecnológicos de la Entidad.
- **Autorización:** se asignarán permisos basados en roles y responsabilidades a todos los colaboradores, operadores o terceros.
- **Registro y control:** se deberá mantener un registro de todas las identidades de colaboradores, operadores y terceros y sus correspondientes requerimientos a través de las solicitudes realizadas en la herramienta de gestión.
- **Monitoreo y reporte:** supervisar el uso de las identidades de colaboradores, operadores y terceros.

PARÁGRAFO 2. El área funcional o dependencias que administren sistemas de información en el ICBF, serán los responsables de establecer las directrices y acciones necesarias que permitan dar cumplimiento a las políticas relacionadas con el control de acceso a los sistemas de información que se encuentran bajo su administración.

PARÁGRAFO 3. 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 4. 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 5. 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 quien validará la solicitud.

ARTÍCULO 8. Política de inteligencia de amenazas. El ICBF, a través de la Dirección de Información y Tecnología, establecerá mecanismos de recolección, análisis y uso de información sobre amenazas cibernéticas, con el fin de proteger los activos de la organización y mitigar los riesgos asociados.

PARÁGRAFO 1. La Dirección de Información y Tecnología utilizará fuentes de información, tanto internas como externas, para recolectar datos sobre amenazas cibernéticas y de seguridad más relevantes para la Entidad.

PARÁGRAFO 2. Los datos recolectados sobre amenazas [vulnerabilidades conocidas, actividad de amenazas actuales entre otras], deben ser socializados con los profesionales encargados de la Dirección de Información y Tecnología y/o Subdirección de Recursos Tecnológicos, con el fin de analizar e identificar patrones, tácticas, técnicas y procedimientos utilizados por diferentes vectores de ataque.

PARÁGRAFO 3. La Dirección de Información y Tecnología implementará sistemas de monitoreo que permitan evaluar en tiempo real actividad de red, detección de intrusiones y otros indicadores de compromisos, incluyendo el seguimiento y monitoreo de logos, eventos de seguridad y vulnerabilidades.

PARÁGRAFO 4. La Dirección de Información y Tecnología en cabeza de la subdirección de recursos tecnológicos deberá realizar evaluaciones periódicas de vulnerabilidades en sistemas y aplicaciones y conforme a los resultados priorizar las actividades de remediación y mitigación.

ARTÍCULO 9. Política de seguridad de la información en la gestión de proyectos. La Dirección de Contratación debe incluir lineamientos en materia de seguridad y privacidad de la información, ciberseguridad y continuidad de la operación en la gestión de proyectos para proteger los datos y asegurar el cumplimiento de las normativas vigentes aplicables. Esto aplica a todos los proyectos gestionados por el ICBF, incluyendo aquellos realizados por colaboradores, proveedores o terceros.

ARTÍCULO 10. Política de seguridad para relación con proveedores. El ICBF establecerá mecanismos de control en relación con sus proveedores o terceros 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 de Calidad.

PARÁGRAFO 1. El representante legal del operador, tercero y proveedor de servicios tecnológicos deberá aceptar y firmar el acuerdo de confidencialidad establecido por el ICBF. Además, es responsabilidad del representante garantizar que todo el personal bajo su cargo firme un documento de compromiso de confidencialidad, asegurando así la protección de la información manejada. Todos estos documentos deberán ser firmados bajo los logos correspondientes del operador, tercero o proveedor de servicios tecnológicos.

PARÁGRAFO 2. Los supervisores de contratos deberán realizar seguimiento, control y revisión de los servicios suministrados por los operadores, proveedores y/o contratistas, con el fin de que propendan por el cumplimiento de las obligaciones establecidas en la Guía de Bienes y Servicios de Calidad.

PARÁGRAFO 3. Los supervisores de contrato deben implementar mecanismos y condiciones con los contratistas y proveedores de servicios tecnológicos para asegurar el cumplimiento del procedimiento de gestión de cambios en los servicios proporcionados a la Entidad.

PARÁGRAFO 4. Los proveedores, operadores y terceros 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.

PARÁGRAFO 5. Está prohibido cualquier manipulación, alteración o cambio de configuraciones, políticas, métricas, estadísticas o datos sensibles en las plataformas, herramientas tecnológicas o sistemas de información de la entidad por parte de los proveedores de servicios de tecnología, operadores o terceros, sin la previa autorización de la Subdirección de Recursos Tecnológicos.

ARTÍCULO 11. Política de gestión de incidentes de seguridad y privacidad de la información o ciberseguridad. El ICBF promoverá entre los colaboradores, proveedores y operadores el reporte de incidentes o eventos de seguridad 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 investigarlos y solucionarlos, 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. Según la criticidad del incidente, la Dirección de Información y Tecnología lo reportará al Equipo Nacional de Respuesta a Emergencias Informáticas (COLCERT), siguiendo los lineamientos y parámetros que este defina. Si el incidente está relacionado con datos personales, se reportará a la Superintendencia de Industria y Comercio (SIC).

ARTÍCULO 12. 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 de los servicios de tecnología 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 lidera 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 con el objeto de propender por la disponibilidad y el acceso a los sistemas, datos y aplicaciones de información críticos en caso de interrupciones o eventos disruptivos.

PARÁGRAFO 4. La Dirección de Información y Tecnología, estructura e implementa un Plan de Continuidad de la Operación Tecnológica enfocados a los aplicativos y servicios en nube y ambientes híbridos cumpliendo con la particularidad técnica que estos demandan, con el fin de proteger los datos de la entidad.

PARÁGRAFO 5. La Dirección de Información y Tecnología implementará una arquitectura de seguridad que incluya la segmentación de redes, el cifrado de datos en tránsito, en reposo, y controles de acceso granulares basados en roles y responsabilidades. Así mismo, adoptará prácticas de monitorización continua y respuesta a incidentes para detectar y mitigar amenazas

de manera proactiva, garantizando que los sistemas de información del ICBF cumplan con las normativas y regulaciones aplicables, cumpliendo con las mejores prácticas de seguridad para entornos de nube híbrida.

ARTÍCULO 13. Política legal y 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.

CAPÍTULO III CONTROLES DE PERSONAS

ARTÍCULO 14. Política de seguridad y privacidad de los recursos humanos: El ICBF, a través de la Dirección de Información y Tecnología y con el apoyo de la Dirección de Gestión Humana, promoverá que los servidores asuman sus responsabilidades en materia de seguridad de la información. Esto tiene como objetivo reducir los riesgos de pérdida, robo, fraude, suplantación de identidad y/o mal uso de los medios tecnológicos de la entidad, asegurando la confidencialidad, disponibilidad e integridad de la información.

PARÁGRAFO 1. La Dirección de Gestión Humana establece lineamientos y procedimientos internos para la selección, vinculación y retiro de colaboradores. Durante estos procesos, se llevan a cabo las verificaciones necesarias para confirmar la legalidad de la información proporcionada por los candidatos al cargo.

PARÁGRAFO 2. La Dirección de Contratación deberá incluir en todos los estudios previos de proyectos o contratos a celebrar cualquiera que sea su modalidad, cláusulas u obligaciones de seguridad y privacidad 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.

CAPÍTULO IV CONTROLES FÍSICOS

ARTÍCULO 15. 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. 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.

PARÁGRAFO 3. 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 16. 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 gestión de 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, mantener, proteger y ejecutar pruebas de restauración periódicas de las 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, siniestros 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 17. Política de seguridad del sistema y de la red. 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 y contractuales, 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 de 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 entidad contratista o con la cual se realiza el convenio.

PARÁGRAFO 3. La Dirección de Información y Tecnología a través de la Subdirección de Recursos Tecnológicos, deberá segmentar la red, estableciendo buenas prácticas en la separación de ambientes 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 18. Política de servicios en la NUBE. La Dirección de Información y Tecnología, a través de la Subdirección de Recursos Tecnológicos será el área encargada de mantener la seguridad y privacidad de la información, así como el uso seguro y eficiente de los servicios de

procesamiento de la información en plataformas de computación en la nube que son utilizadas por el ICBF cumpliendo con los niveles de compromiso y brindando continuidad a la operación de la Entidad.

PARÁGRAFO 1. Para la utilización de servicios de procesamiento en nube "AZURE", no se autoriza el uso de servicios para fines personales. Además, todos los servicios utilizados deben ser aprobados previamente por la Dirección de Tecnología de la Información.

PARÁGRAFO 2. Para la utilización de servicios de almacenamiento en la nube "OneDrive, SharePoint", almacenamiento AZURE, es responsabilidad de cada colaborador garantizar que solo se almacene información de carácter institucional. El uso no autorizado de estos servicios puede resultar en sanciones disciplinarias o llamados de atención por parte del supervisor del contrato.

PARÁGRAFO 3. Los colaboradores serán responsables que la información institucional no se almacene en servicios de nube personales y que se sigan las políticas de seguridad y privacidad establecidas para proteger la información del ICBF.

PARÁGRAFO 4. La Dirección de Información y Tecnología, a través de la Subdirección de Recursos Tecnológicos, será responsable de garantizar que los servicios en la nube cumplan con todas las normativas y regulaciones aplicables, incluyendo aquellas relacionadas con la protección y privacidad de la información de la Entidad y los datos personales. Además, esta área se encargará de supervisar la implementación de medidas de seguridad adecuadas para proteger los datos contra accesos no autorizados, pérdidas o filtraciones. También se asegurará de que los proveedores de servicios en la nube cumplan con los estándares de calidad y seguridad establecidos por la Entidad.

ARTÍCULO 19. 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, ni tampoco se generará backup o copia de 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 deberá desarrollar y/o adquirir 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 deberá establecer 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. El área funcional del software es responsable de realizar y garantizar el registro, actualización y modificación de la información. Asimismo, debe asumir la responsabilidad por la correcta gestión de la información, propendiendo por la integridad de la información; así como responder por las consecuencias derivadas de las modificaciones realizadas en los aplicativos.

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 20. Política de criptografía. La Dirección de Información y Tecnología deberá brindar, de acuerdo con los requerimientos del ICBF, las herramientas que permitan el cifrado de la información para proteger la confidencialidad, integridad y disponibilidad de la información clasificada o reservada.

CAPÍTULO V
RESPONSABILIDADES SOBRE EL USO DE LOS RECURSOS TECNOLÓGICOS.

ARTÍCULO 21. Política de ciberseguridad. Todos los colaboradores, proveedores y operadores de servicios tecnológicos que utilicen los activos de información de la entidad tienen la responsabilidad de cumplir con las políticas establecidas para su uso adecuado. El uso inapropiado de estos recursos puede comprometer la continuidad de la operación y, en consecuencia, el cumplimiento de la misión institucional. Por lo tanto, es crucial que todos los involucrados comprendan y sigan estrictamente las directrices de seguridad y privacidad de la información.

ARTÍCULO 22. 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, el cual se regirá por los siguientes lineamientos:

- La Dirección de Información y Tecnología proporcionará las directrices necesarias para la correcta estructura y creación de usuarios en la cuenta institucional. Estas instrucciones incluirán detalles sobre los nombres de usuario, los permisos de acceso y las configuraciones de seguridad, para asegurar que todos los usuarios tengan acceso adecuado y seguro a los recursos del ICBF. 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 electrónico tienen como sustento normativo 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 para prevenir la pérdida o fuga de información reservada o clasificada, así como accesos no autorizados a la infraestructura tecnológica del ICBF. Estas medidas deben propender por la protección de la confidencialidad, integridad y disponibilidad de la información.
- La Dirección de Información y Tecnología cuenta con políticas para el envío de correos electrónicos de usuarios internos y externos del ICBF:

  Policy ICBF Outbound Users: Los usuarios regulares de la Entidad pueden enviar un máximo de:

  - **150 destinatarios externos** por hora.
  - **500 destinatarios internos** por hora.
  - **650 destinatarios en total** por día.

  Policy ICBF Outbound VIP: Los usuarios con cargos directivos pueden enviar un máximo de:
  - **400 destinatarios externos** por hora.
  - **1000 destinatarios internos** por hora.
  - **1400 destinatarios en total** por día.

  Policy ICBF Outbound Account Services: Esta política aplica a cuentas de servicio utilizadas por las aplicaciones del ICBF y a usuarios o buzones autorizados por los directores de la Entidad para el envío de correos masivos. Estas cuentas permiten el envío de mensajes en alto volumen, exclusivamente para los fines autorizados.
- Está **prohibido el envío de correos masivos a nivel nacional**, tanto internos como externos, por parte de los usuarios regulares del ICBF. Se entiende como correo masivo cualquier envío que exceda los umbrales definidos en la política Policy ICBF Outbound Users.

  Excepciones a esta política:

  El envío de correos masivos está permitido únicamente si se realiza a través de las siguientes dependencias autorizadas:

- Dirección General
- Subdirección General
- Secretaría General
- Oficina Asesora de Comunicaciones
- Dirección de Planeación y Gestión de Control
- Dirección de Gestión Humana
- Dirección de Información y Tecnología

Adicionalmente, los correos enviados desde cuentas que operan bajo la política **ICBF Outbound Account Services** estarán exentos de esta restricción, siempre y cuando su uso haya sido previamente autorizado por los directores responsables, se encuentre alineado con las necesidades operativas de la Entidad y cumpla con los procedimientos establecidos para la asignación de estos permisos.

- En las direcciones regionales está prohibido el envío de correos masivos tanto internos como externos, salvo a través de los Directores Regionales o quien haga las veces de profesional enlace 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 Informática de Soluciones (MIS), la delegación del buzón correspondiente, relacionando los funcionarios o contratistas que podrán escribir o responder en nombre de él.
- Todo correo sospechoso respecto de su remitente o contenido deberá ser inmediatamente reportado a la Mesa Informática de Soluciones (MIS), 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/o de la Dirección de Planeación y Control de Gestión, en caso de cifras oficiales.
- 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.

ARTÍCULO 23. 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.

ARTÍCULO 24. 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. 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.
- 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.

- Los usuarios que no se encuentren vinculados a la Entidad, tendrán su cuenta inhabilitada o inactiva, con un periodo de retención de información almacenada en OneDrive de (180 días), posterior a ello su cuenta e información será eliminada de forma definitiva.
- Las copias de seguridad de la información de los colaboradores deberán ser justificadas y 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.
- Toda información generada, almacenada, procesada o respaldada durante la relación laboral o contractual es de propiedad de la Entidad. Por esta razón, debe ser protegida en todo momento, garantizando su confidencialidad y evitando cualquier fuga de información sensible o datos personales, incluso después de la finalización de la relación laboral o contractual. En consecuencia, cualquier solicitud de copias de seguridad por parte de excolaboradores será rechazada, salvo que exista una autorización expresa de la alta dirección y se cumpla con las disposiciones legales aplicables.
- 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 personal encargado de realizar las activaciones, actualizaciones y desactivaciones de cuentas de usuarios institucionales (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 laboral, administrativo o contractual, 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"*, modificada por la Ley 1915 de 2018; así como a la Decisión 351 de 1993 de la Comunidad Andina de Naciones. Además, deberán cumplir con cualquier otra normativa 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 Dirección de Información y Tecnología debe definir controles para la prevención de intrusos y la protección contra software malicioso.
- La Dirección de Información y Tecnología en cabeza de la Subdirección de Recursos tecnológicos adquirirá un software con características de Detección y respuesta extendidas (XDR), con el fin de dotar a la entidad de una plataforma unificada de incidentes de seguridad que utilice tecnologías de vanguardia como lo son la inteligencia artificial y automatización. Proporcionando de una manera holística y eficaz la protección de los activos de información frente a ciberataques avanzados.
- El manejo de la aplicación de antivirus - antimalware para equipos institucionales a nivel nacional y servidores [instalación, configuración, administración y/o desinstalación] debe ser realizado únicamente por el personal autorizado por la Dirección de Información y Tecnología.
- 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 hubiere asignado, allegando la respectiva denuncia en caso de pérdida o robo le 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 y privacidad de la información o ciberseguridad 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
- Queda estrictamente prohibida la conexión de módems o cualquier otro dispositivo de conexión a la red sin la previa autorización de la Dirección de Información y Tecnología. Esta medida es necesaria para asegurar la integridad y seguridad de la infraestructura tecnológica.
- 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.
- 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.

ARTÍCULO 25. 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, proveedor o tercero debe ser consciente de dar un buen uso a las herramientas de almacenamiento proporcionadas por la Dirección de Información y Tecnología. La información almacenada debe ser estrictamente de carácter institucional, y se deben asegurar los controles de acceso necesarios para proteger la seguridad y privacidad de la información.
- Todo colaborador, proveedor o tercero es responsable del cambio de contraseña de acceso a los sistemas de información o recursos informáticos periódicamente.
- Todo colaborador o proveedor es responsable de los registros y modificaciones de información que se hagan a nombre de su cuenta de usuario.
- Todo colaborador, proveedor o tercero es responsable de los registros y modificaciones de información realizados con su cuenta.

ARTÍCULO 26. Del uso de tecnología emergente.

- La protección de la información en los sistemas o herramientas de software del ICBF que utilicen tecnologías de vanguardia como la inteligencia artificial, deberá contar con controles para mantener la confidencialidad, integridad y disponibilidad de los datos.
- La Subdirección de Recursos Tecnológicos debe fortalecer las medidas de seguridad avanzadas que incluyan, la autenticación multifactorial, la supervisión constante de actividades sospechosas y la actualización regular de nuestros sistemas. Estas medidas buscan mitigar riesgos y proteger los datos contra accesos no autorizados, ataques cibernéticos y pérdidas de información.
- La base la adopción de ambientes tecnológicos que soportan datos y aplicaciones tanto en entornos locales como en la nube pública, requieren de una estrategia de nube híbrida con medidas de seguridad robustas para proteger los datos de la entidad. La Dirección de Información y Tecnología implementará una arquitectura de seguridad que incluya la segmentación de redes, el cifrado de datos en tránsito, en reposo, y controles de acceso granulares basados en roles y responsabilidades, Así mismo, adoptará prácticas de monitorización continua y respuesta a incidentes para detectar y mitigar amenazas de manera proactiva. Garantizando que los sistemas de información del ICBF cumplan con las normativas y regulaciones aplicables, cumpliendo con las mejores prácticas de seguridad para entornos de nube híbrida.

ARTÍCULO 27. 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 VI
REVISIÓN, VIGENCIA Y DEROGATORIA.

ARTÍCULO 28. Revisión. La Política de Seguridad y Privacidad de la Información, Ciberseguridad 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 29. Publicación. A través de la Oficina Asesora de Comunicaciones, **PUBLÍQUESE** el presente acto administrativo en el Diario Oficial, de acuerdo con lo establecido en el artículo 65 de la Ley 1437 de 2011 - Código de Procedimiento Administrativo y de lo Contencioso Administrativo.

ARTÍCULO 30. Vigencia y derogatoria. La presente Resolución rige a partir de la fecha de su publicación en el Diario Oficial y deroga la Resolución No. 414 del 2024.

PUBLÍQUESE, COMUNÍQUESE Y CÚMPLASE
Dada en Bogotá, D.C., a los 2 de Julio de 2025

ASTRID ELIANA CACERES CARDENAS
Directora General

Aprobó: Diana Parra Cardona – Secretaria General
Milton Fabian Forero Melo - Director de Planeación y Control de Gestión
Amalia Pena Russi - Directora de Información y Tecnología (E)
José Miguel Rueda Vásquez- Jefe de Oficina Asesora Jurídica
Revisó: Diana Carolina Baloy – Asesora Direccion General
Laura Carolina Cortés – Abogada Contratista - Dirección General
Alcides Espinosa Ospino – Secretaría General
Ramiro Lozano Arboleda - Contratista Dirección de Información y Tecnología
Fabio Alexander Triana - Contratista - Arquitecto de Seguridad-Dirección de Información y Tecnología
Víctor Manuel Méndez – Abogado Contratista OAJ
Daniel Eduardo Lozano B. - Profesional Especializado OAJ
Elaboró: Teresa Quilindo Sarasti - Contratista (SGSI) Dirección de Información y Tecnología