RESOLUCIÓN No.

"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 3248 de 2025"

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.

RESOLUCIÓN No.

"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 3248 de 2025"

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.

Que 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 Política de Gobierno Digital, regulada en el Decreto 1078 de 2015, modificado por el Decreto 1008 de 2018 y complementado por el Decreto 338 de 2022, reconoce la Seguridad de la Información y la Seguridad Digital como un principio y habilitador transversal para la transformación digital del Estado, orientado a la gestión y mitigación de riesgos, así como a la protección de la confidencialidad, integridad, disponibilidad y privacidad de la información, frente a amenazas internas y externas que puedan afectar los servicios digitales y los activos de información de las entidades públicas. Atendiendo a esta política pública, el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC, mediante la Resolución 02277 de 2025, actualiza el Modelo de Seguridad y Privacidad de la Información – MSPI como el instrumento rector para la gestión integral de la seguridad digital en las entidades públicas del país. Esta actualización incorpora lineamientos robustos alineados con la versión más reciente de la norma internacional ISO/IEC 27001:2022, fortaleciendo la estrategia de seguridad digital estatal y estableciendo mejores prácticas y requisitos técnicos, organizacionales y de gestión para la protección de los activos de información institucionales.

Que el CONPES 4144 de 2025 establece la política nacional para el desarrollo, adopción y uso responsable de la inteligencia artificial en Colombia, promoviendo principios de ética, transparencia, seguridad, protección de datos personales, gestión de riesgos tecnológicos y fortalecimiento de las capacidades institucionales para el uso de tecnologías emergentes en el sector público.

Que el CONPES 3995 de 2020 establece lineamientos para fortalecer la gestión del riesgo digital, la ciberseguridad y la resiliencia institucional frente a amenazas en el entorno digital, orientando a las entidades públicas a fortalecer sus capacidades para la prevención, detección, respuesta y recuperación ante incidentes de seguridad digital.

Que de conformidad con la Ley 1581 de 2012 y sus decretos reglamentarios, en especial el Decreto 1377 de 2013, las entidades públicas deben garantizar la protección de los datos personales que recolecten, almacenen, utilicen o administren en el ejercicio de sus funciones,

RESOLUCIÓN No.

"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 3248 de 2025"

adoptando medidas técnicas, administrativas y organizacionales que aseguren su confidencialidad, integridad y disponibilidad.

Que, en concordancia con esta política pública, las entidades del Estado deben implementar medidas que permitan gestionar los riesgos asociados al uso de tecnologías emergentes, incluida la inteligencia artificial, garantizando la protección de la información, la privacidad de los datos personales, la seguridad digital y la confiabilidad de los sistemas de información que soportan la prestación de los servicios institucionales.

Que, en este contexto, el Instituto Colombiano de Bienestar Familiar – ICBF deberá incorporar dentro de su **Sistema de Gestión de Seguridad de la Información (SGSI)** lineamientos para la gestión segura de tecnologías emergentes, incluyendo inteligencia artificial, analítica de datos y automatización de procesos, asegurando que su adopción se realice bajo criterios de seguridad, ética, transparencia, responsabilidad y protección de los derechos de los ciudadanos.

Que el Decreto 1430 de 2025, mediante el cual se modifica la estructura del Instituto Colombiano de Bienestar Familiar Cecilia de la Fuente de Lleras – ICBF, hace necesario actualizar la Resolución que adopta la Política de Seguridad y Privacidad de la Información, Ciberseguridad y Continuidad de la Operación de la Entidad.
Que en virtud de lo establecido en el numeral 14 del artículo 3 de la Resolución 8650 de 2021, en sesión del 24 de abril de 2026, Comité Institucional de Gestión y Desempeño aprobó la modificación de la Política General de Seguridad y Privacidad de la Información, Ciberseguridad y Continuidad de Operación.

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 3248 del 02 de julio del 2025

En mérito de lo expuesto,

RESUELVE:

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.

RESOLUCIÓN No.

"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 3248 de 2025"

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 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 programas de capacitación, 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.
7. Gestionar de manera integral las vulnerabilidades de seguridad de la información y ciberseguridad que puedan afectar los activos de información, los servicios tecnológicos y la continuidad tecnológica del ICBF, mediante procesos de identificación, análisis, evaluación, priorización, tratamiento y seguimiento, apoyados en evaluaciones periódicas de vulnerabilidades, monitoreo continuo y planes de remediación, con el fin de reducir la superficie de ataque, prevenir la materialización de riesgos y fortalecer la postura de seguridad y la resiliencia institucional.

CAPÍTULO I.
CONTROLES ORGANIZACIONALES

ARTÍCULO 5. Privacidad y tratamiento de la información. Para el tratamiento de la información de los niños, niñas, adolescentes, familias y colaboradores a los 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 Protección de Tratamiento de Datos Personales del ICBF 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.

RESOLUCIÓN No.

"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 3248 de 2025"

PARÁGRAFO 1. Todos los colaboradores, proveedores y terceros que tengan acceso a la información de carácter personal gestionada por la entidad deben proteger la privacidad y la seguridad de dicha información. Esto se logrará asegurando el cumplimiento de las leyes, normas y regulaciones aplicables, y basándose en los principios de transparencia, consentimiento y seguridad.

PARÁGRAFO 2. La Dirección de Tecnologías de la Información implementará controles para limitar el acceso a la información de carácter personal, solo otorgará el acceso a aquellos funcionarios 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 Tecnologías de la Información, 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 Tecnologías de la Información. 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 Tecnologías de la Información, 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 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 Dirección de Tecnologías de la 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 Tecnologías de la Información 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 Tecnologías de la Información quien validará la solicitud.

ARTÍCULO 8. Política de inteligencia de amenazas.
El Instituto Colombiano de Bienestar Familiar – ICBF, a través de la Dirección de Tecnologías de la Información, establecerá mecanismos para la recolección, correlación, análisis y uso de información relacionada con amenazas cibernéticas y vulnerabilidades tecnológicas, con el propósito de anticipar, identificar y gestionar oportunamente los riesgos que puedan afectar la seguridad de la información, la continuidad de la operación y la prestación de los servicios institucionales.

Para tal efecto, se promoverá el monitoreo permanente de fuentes internas y externas de información sobre ciberamenazas, incluyendo alertas de seguridad, reportes de vulnerabilidades, indicadores de compromiso, tendencias de ataque y buenas prácticas emitidas por organismos especializados nacionales e internacionales.

La inteligencia de amenazas permitirá fortalecer la capacidad institucional para prevenir, detectar, responder y recuperarse ante incidentes de seguridad de la información o ciberseguridad, contribuyendo a la protección de los activos de información, la infraestructura tecnológica y los servicios digitales del Instituto.

RESOLUCIÓN No.

"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 3248 de 2025"

La Dirección de Tecnologías de la Información podrá establecer mecanismos de cooperación e intercambio de información con entidades del gobierno, organismos especializados en seguridad digital y proveedores de servicios tecnológicos, con el fin de fortalecer las capacidades de análisis y gestión de amenazas en el marco del Sistema de Gestión de Seguridad de la Información (SGSI) y de la estrategia de seguridad digital de la entidad.

La información obtenida mediante los procesos de inteligencia de amenazas será utilizada para apoyar la gestión de riesgos de seguridad de la información, la mejora continua de los controles de seguridad, la gestión de vulnerabilidades, la toma de decisiones estratégicas en materia de ciberseguridad y la adopción de medidas preventivas y correctivas que permitan reducir la probabilidad e impacto de incidentes de seguridad de la información o ciberseguridad

PARÁGRAFO 1. La Dirección de Tecnologías de la Información utilizará fuentes de información internas y externas, para la recolección de datos relacionados con amenazas cibernéticas, vulnerabilidades, incidentes de seguridad de la información o ciberseguridad y tendencias de ataque, que puedan representar riesgos para los activos de información, la infraestructura tecnológica y los servicios digitales de la Entidad.

PARÁGRAFO 2. La información recolectada sobre amenazas, vulnerabilidades conocidas, actividad de amenazas actuales, indicadores de compromisos y demás datos relevantes deberá ser analizada y socializada con los profesionales de la Dirección de Tecnologías de la Información, con el fin de identificar patrones, tendencias, tácticas, técnicas y procedimientos utilizados por posibles actores o vectores de ataque que puedan afectar la seguridad de la información institucional.

PARÁGRAFO 3. La Dirección de Tecnologías de la Información implementará mecanismos y herramientas de monitoreo y análisis de seguridad que permitan evaluar en tiempo real la actividad de red, detectar posibles intrusiones y analizar indicadores de compromisos, incluyendo el seguimiento y monitoreo de registros (logs), eventos de seguridad, tráfico de red y vulnerabilidades en los sistemas de información

PARÁGRAFO 4. La Dirección de Tecnologías de la Información realizará evaluaciones periódicas de vulnerabilidades en sistemas, aplicaciones e infraestructura tecnológica, con el propósito de identificar debilidades de seguridad y, con base en los resultados obtenidos, priorizar e implementar las acciones de remediación, mitigación y fortalecimiento de los controles de seguridad que correspondan.

ARTÍCULO 9. Política de seguridad de la información en la gestión de proyectos. El Instituto Colombiano de Bienestar Familiar – ICBF, a través de la Dirección de Contratación y en coordinación con la Dirección de Tecnologías de la Información, deberá incorporar lineamientos y requisitos en materia de seguridad y privacidad de la información, ciberseguridad y continuidad de la operación en todas las etapas de la gestión de proyectos institucionales, con el fin de proteger los activos de información, los datos personales y los sistemas de información así como asegurar el cumplimiento de las normativas vigentes aplicables. Este inciso se 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 Tecnologías de la Información, 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.

RESOLUCIÓN No.

"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 3248 de 2025"

PARÁGRAFO 1. El representante legal del operador, tercero o proveedor de servicios tecnológicos deberá suscribir el acuerdo de confidencialidad establecido por el Instituto Colombiano de Bienestar Familiar-ICBF como requisito previo para la prestación del servicio o la ejecución de las actividades contractuales. Además, es responsabilidad del representante legal garantizar que todo el personal o subcontratistas que participen en la ejecución del contrato y que tengan acceso a información de la Entidad, suscriban los respectivos compromisos de confidencialidad, con el fin de asegurar la protección, reserva y adecuado tratamiento de la información institucional.

Los documentos que soporten dichos compromisos deberán quedar debidamente formalizados y firmados, y deberán elaborarse en los formatos propios del operador, tercero o proveedor de servicios tecnológicos, garantizando que cumplan con los lineamientos de confidencialidad y protección de la información definidos por la Entidad.

PARÁGRAFO 2. Los supervisores de contratos deberán realizar el seguimiento, control y verificación de los servicios suministrados por los operadores, proveedores y/o contratistas, con el propósito de garantizar el cumplimiento de las obligaciones contractuales, así como los lineamientos establecidos en la Guía de Bienes y Servicios de Calidad y en las disposiciones institucionales relacionadas con la seguridad y privacidad de la información, la ciberseguridad y la continuidad de la operación

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, sistemas de información, infraestructura o componentes tecnológicos suministrados a la Entidad.

Lo anterior con el propósito de asegurar que cualquier cambio que pueda afectar los activos de información, los servicios tecnológicos, la seguridad de la información o la continuidad de la operación, sea debidamente evaluado, autorizado, documentado e implementado conforme a los lineamientos establecidos por el Instituto Colombiano de Bienestar Familiar – ICBF.

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 Dirección de Tecnologías de la Información.

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 o ciberseguridad 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 de seguridad de la información o ciberseguridad, la Dirección de Tecnologías de la Información lo reportará al Equipo Nacional de Respuesta a Emergencias Informáticas (COLCERT), siguiendo los lineamientos y parámetros que este defina.

RESOLUCIÓN No.

"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 3248 de 2025"

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 Tecnologías la Información, 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 Tecnologías de la Información 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 Tecnologías de la Información, 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.

La Dirección de Tecnologías de la Información 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 Instituto Colombiano de Bienestar Familiar - ICBF velará por la identificación, análisis, documentación, seguimiento y cumplimiento de los requisitos legales regulatorios y contractuales aplicables en materia de seguridad y privacidad de la información, ciberseguridad y protección de datos, en el marco de la normatividad vigente del Estado colombiano.

Para tal efecto, la Entidad garantizará la observancia de las disposiciones relacionadas, entre otros, con derechos de autor y propiedad intelectual, protección de datos personales, transparencia y acceso a la información pública, así como las demás normas aplicables que regulen el manejo, tratamiento, custodia y protección de la información institucional. Estos requisitos deberán estar identificados, actualizados y gestionados en la Matriz de Requisitos Legales del ICBF, la cual permitirá realizar el seguimiento al cumplimiento de la normativa aplicable y establecer las acciones necesarias para su adecuada implementación en el marco del Sistema de Gestión de Seguridad de la Información – SGSI.

CAPÍTULO II CONTROLES DE PERSONAS

ARTÍCULO 14. Política de seguridad y privacidad de los recursos humanos: El ICBF, a través de la Dirección de Tecnologías de la Información y con el apoyo de la Dirección de Talento Humano, promoverá que los funcionarios asuman sus responsabilidades en materia de seguridad y privacidad de la información o ciberseguridad. Esto tiene como objetivo reducir los riesgos de

RESOLUCIÓN No.

"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 3248 de 2025"

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 Talento Humano 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.

ARTÍCULO 15. Política de Teletrabajo Cuando los funcionarios del Instituto Colombiano de Bienestar Familiar – ICBF desarrollen sus funciones bajo modalidades de teletrabajo, deberán cumplir con los lineamientos institucionales de seguridad y privacidad de la información, ciberseguridad y uso adecuado de los recursos tecnológicos definidos por la Entidad. En este sentido, deberán adoptar las medidas necesarias para garantizar la protección de la información institucional, el uso seguro de los equipos y redes de comunicación, así como evitar el acceso no autorizado, la divulgación indebida o la pérdida de información durante el desarrollo de sus actividades fuera de las instalaciones de la Entidad. La Dirección de Tecnologías de la Información, en coordinación con la Dirección de Talento Humano, podrá establecer lineamientos, controles y buenas prácticas para el acceso seguro a los sistemas de información y el uso de dispositivos tecnológicos en entornos de trabajo remoto, con el fin de mitigar los riesgos asociados a esta modalidad de trabajo.

ARTÍCULO 16. Conciencia y cultura de seguridad de la información: El Instituto Colombiano de Bienestar Familiar – ICBF promoverá el fortalecimiento de la cultura de seguridad y privacidad de la información, ciberseguridad y protección de datos personales entre los funcionarios, contratistas y proveedores de la Entidad, a través de estrategias de sensibilización, capacitación y divulgación de buenas prácticas contempladas en el Plan de Cambio y cultura

CAPÍTULO III CONTROLES FÍSICOS

ARTÍCULO 17. 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.

RESOLUCIÓN No.

"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 3248 de 2025"

ARTÍCULO 18. Protección de centros de datos y seguridad ambiental, El Instituto Colombiano de Bienestar Familiar – ICBF implementará medidas de seguridad física y ambiental para la protección de los centros de datos, salas técnicas y demás instalaciones que alberguen infraestructura tecnológica crítica, con el fin de garantizar la disponibilidad, integridad y confidencialidad de los activos de información. En este sentido, la Entidad establecerá controles orientados a prevenir, detectar y mitigar riesgos asociados a accesos físicos no autorizados, fallas en el suministro eléctrico, incendios, inundaciones, variaciones de temperatura, humedad y demás condiciones ambientales que puedan afectar el funcionamiento de los sistemas de información y de la infraestructura tecnológica. La Dirección de Tecnologías de la Información, en coordinación con las dependencias competentes, definirá e implementará los controles necesarios para la protección física y ambiental de los centros de datos, incluyendo controles de acceso físico, sistemas de monitoreo, suministro eléctrico regulado, sistemas de detección y extinción de incendios, control de temperatura y humedad, así como procedimientos para la gestión segura de los equipos tecnológicos.

ARTÍCULO 19. Eliminación o disposición segura de equipos: La Dirección de Tecnologías de la Información antes de la disposición final, reutilización o baja de equipos tecnológicos y medios de almacenamiento, deberá realizar la eliminación segura de la información contenida en dichos dispositivos, mediante procedimientos que garanticen la imposibilidad de recuperación de la información.

ARTÍCULO 20. Control de acceso a áreas seguras, el acceso a las áreas seguras del Instituto Colombiano de Bienestar Familiar – ICBF, tales como centros de cableado y datacenter o espacios donde se procese o almacene información crítica, deberá estar restringido únicamente al personal autorizado y debidamente identificado. La Entidad implementará mecanismos de control de acceso físico, tales como bitácoras de ingreso, cerraduras de seguridad, tarjetas de acceso, registros de ingreso, sistemas biométricos u otros controles que permitan verificar, registrar y monitorear el ingreso y permanencia en dichas áreas.

ARTÍCULO 21. Protección de equipos tecnológicos: La Dirección de Tecnologías de la Información implementará medidas para proteger los equipos y la infraestructura tecnológicos que soporta los sistemas de información frente a riesgos físicos, ambientales o de manipulación no autorizada. En este sentido, se deberán adoptar controles para la ubicación segura de los equipos, su adecuada instalación, mantenimiento y protección frente a amenazas tales como daños físicos, robo, vandalismo o condiciones ambientales inadecuadas.

CAPÍTULO IV
RESPONSABILIDADES SOBRE EL USO DE LOS RECURSOS TECNOLÓGICOS.

ARTÍCULO 22. Política de seguridad de las operaciones. La Dirección de Tecnologías de la Información, será la encargada de la operación y administración de la plataforma tecnológica que soporta la operación del ICBF. En desarrollo de esta responsabilidad, deberá garantizar la **implementación y** funcionamiento de controles de seguridad en la operación de los sistemas de información, la infraestructura tecnológica y los servicios asociados, con el propósito de proteger la confidencialidad, integridad y disponibilidad de la información institucional. La Dirección de Tecnologías de la Información, deberá asegurar que los cambios realizados sobre la infraestructura tecnológica, sistemas de información y servicios tecnológicos se gestionen de manera controlada, conforme a los procedimientos institucionales de gestión de cambios y con las autorizaciones correspondientes.
De igual manera, deberá implementar mecanismos de gestión y monitoreo de la capacidad de los recursos tecnológicos, con el fin de garantizar que la infraestructura tecnológica, los sistemas de información y los servicios digitales dispongan de la capacidad de procesamiento, almacenamiento y disponibilidad necesarios para soportar la operación del ICBF, realizando análisis periódicos, proyecciones de crecimiento y provisión de recursos tecnológicos de acuerdo con las necesidades actuales y futuras de la Entidad

RESOLUCIÓN No.

"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 3248 de 2025"

PARÁGRAFO 1. La Dirección de Tecnologías de la Información, 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, 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 Dirección de Tecnologías de la Información, en conjunto con los líderes de proceso.

PARÁGRAFO 3. La Dirección de Tecnologías de la Información deberá implementar mecanismos de monitoreo y análisis del desempeño de la infraestructura tecnológica y de los sistemas de información, que permitan identificar oportunamente situaciones de saturación, degradación del servicio o limitaciones de capacidad, con el fin de adoptar medidas preventivas que aseguren la continuidad de los servicios tecnológicos y la disponibilidad de la información institucional.

ARTÍCULO 23. Política de seguridad del sistema y de la red. La Dirección de Tecnologías de la Información, establecerá los mecanismos necesarios para proveer la disponibilidad de las redes y de los servicios que dependen de ellas y dispondrá y monitoreará los mecanismos necesarios de seguridad 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 Tecnologías de la Información 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 24. Política de seguridad para la adquisición, desarrollo y mantenimiento de sistemas. La Dirección de Tecnologías de la 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 Tecnologías de la Información será la única dependencia de la Entidad autorizada para adquirir, desarrollar, implementar, avalar la adquisición y recepción de

RESOLUCIÓN No.

"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 3248 de 2025"

sistemas de información o software requeridos para apoyar los procesos de la Sede de la Dirección General del Instituto Colombiano de Bienestar Familiar – ICBF, en coordinación con el área o dependencia que identifique la necesidad del software, 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 Tecnologías de la Información, 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 Tecnologías de la Información deberá propender por que los sistemas de información o aplicativos incluyan controles de seguridad y cumplan con las políticas de seguridad de la información.

PARÁGRAFO 4. Previo a la aprobación y puesta en producción de nuevos sistemas y/o actualizaciones, la Dirección de Tecnologías de la Información deberá realizar pruebas funcionales, técnicas y de seguridad en ambientes de pruebas, para validar su operatividad, el cumplimiento de los requerimientos definidos y los lineamientos institucionales en materia de seguridad y privacidad de la información y ciberseguridad.

De igual manera, los desarrollos deberán contemplar pruebas funcionales, técnicas y de seguridad antes de su puesta en producción, garantizando que los sistemas cumplan con los requerimientos definidos y con los lineamientos institucionales en materia de seguridad y privacidad de la información y ciberseguridad.

PARÁGRAFO 5. Los sistemas de información desarrollados o adquiridos por la Entidad deberán contar con la documentación técnica y funcional correspondiente, de acuerdo con los lineamientos establecidos en, el procedimiento P6.GTI Procedimiento Para Desarrollo y Mantenimiento de Sistemas de Información . Esta incluirá como mínimo, la descripción de los requerimientos, arquitectura del sistema, y manuales técnicos, de instalación y configuración, Las versiones de los desarrollos de software deberán gestionarse y preservarse mediante mecanismos de control de versiones y repositorios institucionales, asegurando su trazabilidad, integridad y disponibilidad para futuras actualizaciones, auditorías, mantenimiento o recuperación ante incidentes.

PARÁGRAFO 6. 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 Tecnologías de la Información, para su correcto funcionamiento y protección de la información.

PARÁGRAFO 7. La Dirección de Información y Tecnología implementará controles técnicos y herramientas tecnológicas que permitan restringir, controlar y monitorear la instalación de software no autorizado o que no se encuentre aprobado dentro de la línea base de los activos de información del ICBF. Para tal efecto, se deberán establecer mecanismos de gestión de aplicaciones autorizadas, control de privilegios de instalación, listas blancas de software, monitoreo de integridad de los equipos y verificación periódica del cumplimiento de la línea base de configuración, cualquier instalación de software deberá contar con la validación previa del área competente de tecnología, garantizando que el aplicativo cumpla con los requisitos técnicos, de licenciamiento, compatibilidad y seguridad de la información definidos por la Entidad

PARÁGRAFO 8. El software que se adquiera a través de proyectos, programas, contratos o convenios deberá incorporar lineamientos para la supervisión, control y seguimiento a las actividades de desarrollo, implementación y entrega de los productos contratados. Dichos lineamientos deberán establecerse en las cláusulas contractuales, términos de referencia y/o especificaciones técnicas, e incluir aspectos relacionados con el cumplimiento de requisitos funcionales, técnicos y de seguridad de la información, la entrega de documentación técnica y funcional, la gestión de versiones, las pruebas de aceptación, la transferencia de conocimiento y propiedad del código fuente cuando aplique. Asimismo, se deberá garantizar que los desarrollos realizados por terceros cumplan con los estándares, lineamientos de arquitectura tecnológica y

políticas de seguridad de la información definidas por la Entidad, permitiendo la adecuada administración, mantenimiento, respaldo y continuidad de los sistemas de información.

PARÁGRAFO 9. El área funcional responsable del software deberá solicitar y /o autorizar la baja, desinstalación o retiro del software que presente obsolescencia tecnológica o no se encuentren en uso, y con base en dicha solicitud o autorización, la Dirección de Tecnologías de la Información, será responsable de ejecutar las acciones técnicas y administrativas necesarias para la desinstalación, actualización de inventarios, gestión de licenciamiento y el adecuado control de los activos de software de la Entidad.

PARÁGRAFO 10. La Dirección de Tecnologías de la información, deberá definir e implementar métodos, lineamientos y/o técnicas para el desarrollo de software seguro, los cuales deberán que incorporen y requisitos de seguridad de la información y buenas prácticas de desarrollo seguro y que sean aplicables de manera clara, estandarizada durante todo el ciclo de vida del desarrollo del software. Cuando los desarrollos de software sean realizados por dependencias diferentes a la Dirección de Tecnologías de la Información, estos deberán cumplir con los lineamientos, estándares técnicos, requisitos funcionales y requisitos de seguridad de la información definidos por la DTI, dichos desarrollos deberán ser sometidos a procesos de revisión, validación y aprobación técnica antes de su implementación o puesta en producción.
En caso de que los desarrollos no cumplan con los lineamientos, estándares o requisitos establecidos, la Dirección de Tecnologías de la Información no procederá con su recepción, integración o puesta en funcionamiento dentro de la infraestructura tecnológica de la Entidad, hasta tanto se realicen los ajustes, validaciones y entrega de la documentación correspondiente.
.

ARTÍCULO 25. Política de criptografía. La Dirección de Tecnologías de la Información 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.

ARTÍCULO 26. 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 27. 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 Tecnologías de la Información 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.

RESOLUCIÓN No.

"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 3248 de 2025"

- 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 Tecnologías de la Información 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 Tecnologías de la Información 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:

  - **250 destinatarios externos** por hora.
  - **500 destinatarios internos** por hora.
  - **500 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 Control de Gestión
- Dirección de Talento Humano
- Dirección de Tecnologías de la Información

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.

RESOLUCIÓN No.

"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 3248 de 2025"

- 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.
- Todos los colaboradores, contratistas y proveedores que hagan uso del correo electrónico institucional deberán reportar de manera inmediata cualquier mensaje sospechoso de fraude, suplantación, enlaces maliciosos o archivos adjuntos no solicitados, utilizando la herramienta habilitada en el cliente de correo electrónico institucional. Para ello, deberán hacer clic derecho sobre el mensaje y seleccionar la opción "Informar- Reportar como phishing", lo cual permitirá su envío automático al equipo responsable de la gestión de seguridad de la información para su análisis y tratamiento. En ningún caso el usuario deberá abrir enlaces, descargar archivos adjuntos, responder o interactuar con el contenido del mensaje sospechoso antes de realizar el reporte, ya que esto podría facilitar la materialización de incidentes de seguridad de la información. El uso de esta funcionalidad automatizada permite reducir el riesgo asociado a ataques de phishing, proteger los activos de información de la Entidad y fortalecer los mecanismos de detección y respuesta ante amenazas cibernéticas.
- 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.
- Cuando se trate de cifras oficiales, datos institucionales o información consolidada del ICBF, está expresamente prohibido divulgar, distribuir o compartir dicha información con otras entidades, ciudadanos o terceros, sin la debida autorización de la Alta Dirección y/o del Oficial de Tratamiento de Datos Personales, según corresponda. Toda divulgación de información deberá realizarse conforme a los lineamientos institucionales de manejo de la información, protección de datos personales y transparencia, garantizando que la información sea verificada, autorizada y publicada a través de los canales oficiales definidos por la Entidad.
- El correo electrónico institucional en sus mensajes deberá contener una sentencia de confidencialidad, que será diseñada por la Dirección de Tecnologías de la Información la cual se reflejará en todos los buzones con dominio @icbf.gov.co.
- 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 Tecnologías de la Información, 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 Talento Humano a la Dirección de Tecnologías de la Información, así como a todos los servicios y accesos a sistemas de información de la Entidad o de terceros operados en la Entidad.
- La Dirección de Tecnologías de la Información 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 28. Del uso de internet: La Dirección de Tecnologías de la Información establecerá controles de navegación definidos en la Guía de Políticas de Navegación, los cuales estarán basados en categorías de acceso a contenidos web y deberán ser implementados a través de las herramientas tecnológicas dispuestas por la Entidad para la gestión y control del acceso a Internet. De igual manera, será responsabilidad de todos los colaboradores, contratistas y proveedores que hagan uso de los recursos tecnológicos institucionales deberán cumplir con las directrices, lineamientos y políticas de seguridad y privacidad de la información definidas por la Entidad, garantizando el uso adecuado, responsable y seguro de los servicios de navegación y de los activos de información institucionales, conforme a las disposiciones establecidas en la presente política y demás documentos asociados.

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 29. 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 Tecnologías de la Información.
- 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 Tecnologías de la Información. 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 Tecnologías de la 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.

RESOLUCIÓN No.

"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 3248 de 2025"

- 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 Tecnologías de la Información, 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 Tecnologías de la Información debe definir controles para la prevención de intrusos y la protección contra software malicioso.
- La Dirección de Tecnologías de la Información 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 o ciberseguridad 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 Tecnologías de la Información.
- La única dependencia autorizada para trasladar los elementos y recursos tecnológicos de un puesto a otro será la Dirección de Tecnologías de la Información 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 Tecnologías de la Información 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 Tecnologías de la Información 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 Tecnologías de la Información. 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 Tecnologías de la Información
- La conexión a la red wifi institucional para funcionarios deberá ser administrada desde la Dirección de Tecnologías de la Información 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 Tecnologías de la Información.
- 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.

RESOLUCIÓN No.

"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 3248 de 2025"

- 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 30. 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.

- Con el fin de fortalecer la seguridad de la información, el cambio de contraseña para todos los colaboradores, contratistas y usuarios con acceso a los sistemas de información será forzado cada ciento ochenta (180) días, conforme a los lineamientos de control de acceso definidos en el Sistema de Gestión de Seguridad de la Información (SGSI).
-
- Todo colaborador, proveedor o tercero debe ser consciente de dar un buen uso a las herramientas de almacenamiento proporcionadas por la Dirección de Tecnologías de la Información. 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 31. Política de servicios en la NUBE. La Dirección de Tecnologías de la Información, será la responsable de gestionar, administrar y supervisar el uso seguro de los servicios de computación en la nube utilizados por el Instituto Colombiano de Bienestar Familiar, garantizando la seguridad y privacidad de la información institucional, así como la continuidad de los servicios tecnológicos que soportan la operación de la Entidad. –En este sentido, deberá asegurar que los servicios de procesamiento, almacenamiento y gestión de información en plataformas de computación en la nube se utilicen de forma segura, eficiente y conforme a los lineamientos institucionales, cumpliendo con los niveles de servicio establecidos, los requisitos de seguridad de la información y la normativa vigente aplicable.

PARÁGRAFO 1. La utilización de servicios de computación en la nube institucionales, tales como Microsoft Azure, deberá destinarse exclusivamente para fines institucionales. En consecuencia, no se autoriza el uso de estos servicios para actividades personales. Todo servicio o recurso tecnológico que se pretenda implementar en la plataforma de nube institucional deberá contar con la aprobación previa de la Dirección de Tecnologías de la Información

PARÁGRAFO 2. Para el uso de servicios de almacenamiento en la nube institucional, tales como Microsoft OneDrive, Microsoft SharePoint y los servicios de almacenamiento asociados a Microsoft Azure, los colaboradores serán responsables de garantizar que únicamente se almacene información de carácter institucional, conforme a las políticas de seguridad y privacidad de la información definidas por la Entidad.

PARÁGRAFO 3. Los colaboradores del ICBF deberán abstenerse de almacenar, procesar o compartir información institucional en servicios de nube personales o no autorizados por la Entidad, con el fin de evitar riesgos asociados a la pérdida, filtración o acceso no autorizado a la información institucional.

RESOLUCIÓN No.

"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 3248 de 2025"

PARÁGRAFO 4. La Dirección de Tecnologías de la Información, será responsable de verificar que los servicios en la nube utilizados por la Entidad cumplan con los requisitos de seguridad de la información, privacidad de datos, continuidad de los servicios y normatividad vigente aplicable. La Entidad deberá supervisar la implementación de controles de seguridad adecuados, tales como mecanismos de autenticación, control de accesos, monitoreo de seguridad y gestión de incidentes, con el fin de proteger la información institucional frente a accesos no autorizados, pérdida, alteración o divulgación indebida Igualmente, se deberá asegurar que los proveedores de servicios en la nube cumplan con los estándares de seguridad, calidad y niveles de servicio definidos por el ICBF, así como con las obligaciones contractuales establecidas para la protección de la información institucional y los datos personales.

PARÁGRAFO 5. La información institucional que sea almacenada, procesada o gestionada en servicios de computación en la nube deberá clasificarse y tratarse de acuerdo con los lineamientos institucionales de clasificación y manejo de la información, garantizando que los niveles de protección aplicados correspondan a su grado de confidencialidad, criticidad e impacto para la Entidad. En consecuencia, los responsables de la información deberán asegurar que la información sensible, confidencial o que contenga datos personales cuente con las medidas de seguridad necesarias, tales como controles de acceso, cifrado y mecanismos de protección definidos por el ICBF.

PARÁGRAFO 6. El acceso a los servicios de computación en la nube institucional deberá realizarse únicamente a través de los mecanismos de autenticación y control de acceso definidos por la Entidad, garantizando que cada usuario cuente con los permisos estrictamente necesarios para el cumplimiento de sus funciones. La Dirección de Tecnologías de la Información, será responsable de gestionar, revisar y controlar los accesos a los recursos en la nube, con el fin de prevenir accesos no autorizados y reducir los riesgos asociados al uso indebido de la información institucional.

ARTÍCULO 32. Política de Gestión de Configuración de Activos Tecnológicos

La Dirección de Tecnologías de la Información deberá establecer y mantener procedimientos para la gestión y control de la configuración de los activos tecnológicos de la Entidad, incluyendo sistemas de información, infraestructura tecnológica, dispositivos de red, servicios en la nube y estaciones de trabajo.

Esta gestión deberá garantizar que:

- Las configuraciones de los activos tecnológicos se encuentren documentadas y estandarizadas.
- Se mantenga una línea base de configuración segura para los sistemas y plataformas institucionales.
- Cualquier cambio en la configuración de los activos tecnológicos se realice conforme al procedimiento de gestión de cambios definido por la Entidad.
- Se realicen revisiones periódicas de las configuraciones con el fin de identificar desviaciones, vulnerabilidades o configuraciones no autorizadas.

La Dirección de Tecnologías de la Información será responsable de definir, implementar y supervisar los mecanismos de control que garanticen la integridad, trazabilidad y seguridad de las configuraciones de los activos tecnológicos del ICBF

ARTÍCULO 33. Gestión de vulnerabilidades de seguridad de la información: La Dirección de Tecnologías de la Información deberá establecer e implementar mecanismos para la identificación, análisis, evaluación y tratamiento de vulnerabilidades de seguridad que puedan afectar los activos de información, sistemas de información, infraestructura tecnológica y servicios digitales de la Entidad. De igual manera, se deberán realizar evaluaciones periódicas de vulnerabilidades mediante herramientas automatizadas o revisiones técnicas especializadas, con el propósito de detectar debilidades que puedan ser explotadas por amenazas internas o externas. Las vulnerabilidades identificadas deberán ser analizadas, priorizadas de acuerdo con

su nivel de riesgo y gestionadas oportunamente mediante la aplicación de controles correctivos, mitigaciones o actualizaciones de seguridad que reduzcan la exposición de la Entidad a incidentes de seguridad de la información.

ARTÍCULO 34. Gestión de cambios en activos tecnológicos: La Dirección de Tecnologías de la Información deberá implementar un procedimiento formal para la gestión de cambios que afecten los sistemas de información, infraestructura tecnológica, servicios digitales y demás activos tecnológicos de la Entidad, con el fin de garantizar que dichos cambios se realicen de manera controlada, documentada y autorizada. Todo cambio que pueda impactar la disponibilidad, integridad o confidencialidad de la información deberá ser previamente evaluado, aprobado y registrado conforme a los lineamientos establecidos por la Entidad. Asimismo, deberán realizarse pruebas, validaciones y planes de reversión cuando corresponda, con el propósito de minimizar riesgos operativos o de seguridad derivados de la implementación de cambios en los entornos tecnológicos.

ARTÍCULO 35. Gestión de parches y actualizaciones de seguridad: La Dirección de Tecnologías de la Información deberá garantizar la implementación de un proceso de gestión de parches y actualizaciones de seguridad para los sistemas operativos, aplicaciones, bases de datos, dispositivos de red y demás componentes de la infraestructura tecnológica de la Entidad. Este proceso deberá asegurar la identificación oportuna de actualizaciones y parches de seguridad emitidos por los fabricantes, su evaluación técnica, priorización según el nivel de criticidad y su aplicación en los activos tecnológicos dentro de tiempos razonables que reduzcan el riesgo de explotación de vulnerabilidades conocidas. Las actividades de actualización deberán ser registradas y monitoreadas, garantizando la estabilidad y continuidad de los servicios tecnológicos institucionales.

ARTÍCULO 36. Del uso de tecnología emergente. El uso, adopción o implementación de tecnologías emergentes tales como inteligencia artificial, automatización, analítica avanzada, servicios en la nube, internet de las cosas (IoT) u otras tecnologías digitales innovadoras dentro de la Entidad deberá realizarse bajo criterios de seguridad de la información, gestión de riesgos, protección de datos personales y cumplimiento de la normatividad vigente.

La Dirección de Tecnologías de la Información deberá evaluar previamente los riesgos asociados a la implementación de estas tecnologías, garantizando la aplicación de controles de seguridad adecuados, la protección de los activos de información y la continuidad de los servicios institucionales.

Así mismo, los colaboradores, contratistas y terceros que hagan uso de tecnologías emergentes en el desarrollo de sus funciones deberán cumplir con las políticas, lineamientos y controles definidos por la Entidad en materia de seguridad de la información, protección de datos y uso adecuado de los recursos tecnológicos.
La adopción de estas tecnologías deberá contribuir al fortalecimiento de los procesos institucionales, asegurando que su utilización no comprometa la confidencialidad, integridad y disponibilidad de la información.

ARTÍCULO 37. 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 V
MEJORA, REVISIÓN, VIGENCIA Y DEROGATORIA.

ARTÍCULO 38. Mejora continua del SGSI. El Instituto Colombiano de Bienestar Familiar – ICBF garantizará la mejora continua del Sistema de Gestión de Seguridad de la Información mediante la evaluación periódica de riesgos, auditorías internas, seguimiento a incidentes de

RESOLUCIÓN No.

"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 3248 de 2025"

seguridad, revisión de controles y actualización permanente de la política conforme a cambios tecnológicos, normativos y organizacionales.

ARTÍCULO 39. 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 Tecnologías de la Información, y revisado por el Comité Institucional de Gestión y Desempeño.

ARTÍCULO 40. Publicación. A través de la Oficina Asesora de Comunicaciones, PUBLÍQUESE el presenta 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 41. Vigencia y derogatoria. La presente Resolución rige a partir de la fecha de su publicación, deroga la Resolución No. 3248 del 2025, así como todas aquellas disposiciones que le sean contrarias.

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

ASTRID ELIANA CACERES CARDENAS
Directora General

Aprobó: Diana Parra Cardona – Secretaria General _____
Milton Fabian Forero Melo - Director de Planeación y Control de Gestión_____
Amalia Penna Russi - Director de Tecnologías de la Información_____
José Miguel Rueda Vásquez- Jefe de Oficina Asesora Jurídica (E)_____

Revisó: Diana Carolina Baloy – Asesora Dirección General _____
Laura Carolina Cortés – Abogada Contratista – Dirección General
Alcides Espinosa Ospino – Secretaría General _____
Dirección de Planeación _____
Daniel Eduardo Lozano B. - Profesional Especializado OAJ _____

Elaboró: Teresa Quilindo Sarasti - Contratista (SGSI) Dirección de Tecnologías de la Información_____