PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN, CIBERSEGURIDAD Y CONTINUIDAD DE LA OPERACIÓN

2026

Dirección de Tecnologías de la Información

TABLA DE CONTENIDO

INTRODUCCIÓN

La gestión de Riesgos de Seguridad y Privacidad de la Información, Ciberseguridad y Continuidad de la Operación constituye un proceso esencial para la protección de los activos de información y la resiliencia operativa del Instituto Colombiano de Bienestar Familiar – ICBF. A través de esta gestión, la Entidad identifica, analiza, valora y trata los riesgos que podrían afectar la prestación de sus servicios misionales, el logro de sus objetivos estratégicos y la protección integral de los derechos de los niños, niñas, adolescentes, familias y colaboradores del ICBF.
El Plan de Tratamiento de Riesgos se configura como una herramienta estratégica que orienta la toma de decisiones y define las acciones necesarias para mitigar, evitar, transferir o aceptar el riesgo que superan los niveles de tolerancia definidos por la Entidad. Este plan busca minimizar la probabilidad y el impacto de eventos de seguridad que puedan comprometer la confidencialidad, integridad, disponibilidad y privacidad de los datos de la Entidad

La implementación del presente Plan contribuye al cumplimiento de los lineamientos institucionales y normativos en materia de seguridad digital, promoviendo una cultura de prevención, anticipación y respuesta oportuna frente a incidentes que puedan materializarse, y fortaleciendo así la seguridad de la información en la Entidad.

Lo anterior se enmarca en las disposiciones del Documento CONPES 3995 de 2020 (Política Nacional de Confianza y Seguridad Digital), el Decreto 338 de 2022, que establece el Modelo de Gobernanza de Seguridad Digital en Colombia, y el Decreto Único Reglamentario del Sector TIC (Decreto 1078 de 2015). Asimismo, se da cumplimiento a los lineamientos del Ministerio TIC, en especial a la Resolución 02277 del 3 de junio de 2025, mediante la cual se actualiza el Modelo de Seguridad y Privacidad de la Información – MSPI.

El Plan adopta además las buenas prácticas y lineamientos internacionales establecidos en los estándares ISO/IEC 27001:2022, ISO 31000:2018, ISO/IEC 27005:2022 que proporciona directrices para la gestión del riesgo de seguridad de la información y la Guía para la Gestión Integral del Riesgo en Entidades Públicas – Versión 7 del Departamento Administrativo de la Función Pública (DAFP).

En cumplimiento de lo dispuesto en el Decreto 612 de 2018, se actualiza el presente Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, Ciberseguridad y Continuidad de la Operación, garantizando su alineación con el ciclo de planeación institucional y las obligaciones de mejora continua.

1. OBJETIVO GENERAL

Establecer las acciones, responsabilidades y lineamientos necesarios para implementar el tratamiento de los riesgos de Seguridad y Privacidad de la Información, Ciberseguridad y Continuidad de la Operación en el ICBF, con el fin de mitigar, evitar, transferir o aceptar los riesgos, garantizando la protección de los activos de información, la continuidad de los servicios misionales y el cumplimiento de la normativa vigente en materia de seguridad digital.

1.1 Objetivos Específicos

- Fortalecer el proceso de identificación, análisis, valoración, manejo, monitoreo y tratamiento de los riesgos de Seguridad y Privacidad de la Información, Ciberseguridad y Continuidad de la Operación, asegurando la aplicación efectiva de la metodología institucional y la gestión oportuna de los planes de tratamiento que permitan reducir la exposición de la Entidad a eventos que puedan afectar la operación y la protección de la información.

- Desarrollar estrategias que promuevan el fortalecimiento de competencias, la apropiación de buenas prácticas y la sensibilización de los colaboradores frente a la gestión del riesgo, con el propósito de consolidar una cultura organizacional orientada a la prevención, la protección de los activos de información del ICBF y la garantía de la confidencialidad, integridad y disponibilidad de la información institucional.

2. ALCANCE

La gestión de Riesgos de Seguridad y Privacidad de la Información, Ciberseguridad, y Continuidad de la Operación, Inicia con la Socialización de la Guía de Gestión de Riesgos y Peligros en lo relacionado con seguridad de la información y finaliza fortaleciendo la identificación, análisis, valoración y manejo de los riesgos de seguridad de la información en la Gestión de Proyectos de TI, aplica en los procesos de la Sede de la Dirección General y las 33 regionales del ICBF.

3. DESARROLLO

La gestión de riesgo es una actividad que está inmersa en las actividades del modelo de operación por procesos de la Entidad, la gestión de proyectos y la gestión de cambios, alineándose a los roles y responsabilidades definidos en la Resolución 11980 del 2019 “Por la cual se adopta el Modelo de Planeación y Sistema Integrado de Gestión del ICBF”.

Para el desarrollo del plan de tratamiento de riesgos el ICBF ha establecido la G3.MI Guía de Riesgos y Peligros, la cual presenta los lineamientos para poder identificar, analizar, valorar,

manejar y monitorear los riesgos de Seguridad y Privacidad de la Información, Ciberseguridad y Continuidad de la Operación en los procesos de la Sede de la Dirección General y las 33 regionales del ICBF.

El análisis del riesgo busca establecer la probabilidad de ocurrencia de los riesgos y el impacto de sus consecuencias, calificándolos y evaluándolos con el objeto de obtener información para establecer el nivel de riesgo y las posibles acciones a implementar.

Los riesgos con nivel de criticidad baja podrán ser asumidos o aceptados por decisión del líder del proceso, siempre que todas sus causas cuenten con controles implementados que justifiquen y garanticen su permanencia en dicho nivel. No obstante, estos riesgos deben mantenerse bajo monitoreo periódico para asegurar que su probabilidad e impacto no se incrementen y que los controles asociados continúen siendo eficaces. Así mismo, se debe realizar seguimiento continuo a estos riesgos a través de la gestión de incidentes de seguridad y privacidad de la información o de ciberseguridad, con el fin de identificar posibles materializaciones que puedan modificar su nivel de riesgo y requerir la actualización de los controles o de su plan de tratamiento.

Para la ejecución del plan de tratamiento de Riesgos de Seguridad y Privacidad de la información, Ciberseguridad y Continuidad de la Operación, se realizarán las actividades acordes a lo establecido en el Plan de Seguridad, Ciberseguridad y Privacidad de la Información.

3.1 Responsabilidades

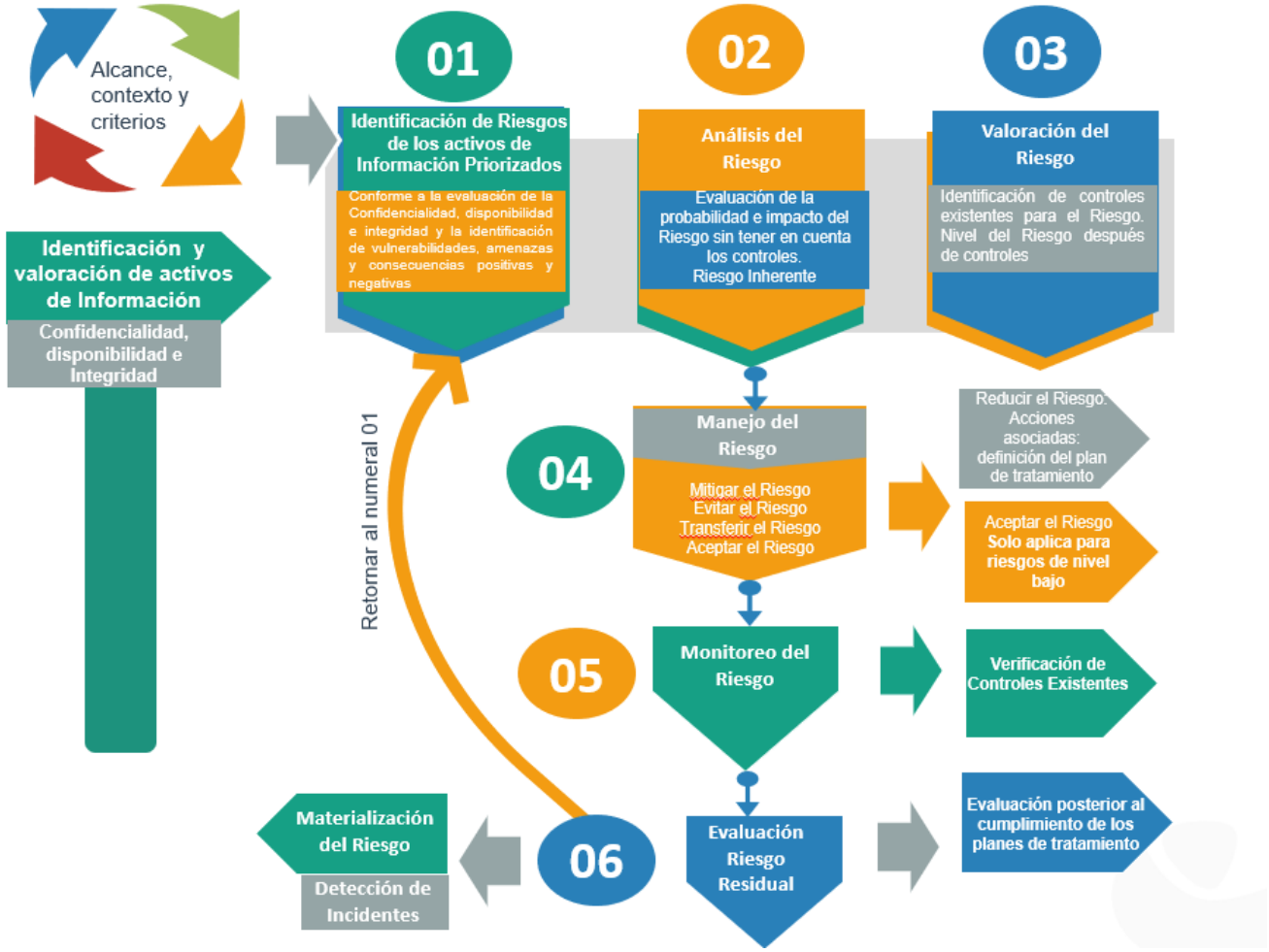
El ICBF deberá definir los roles y responsabilidades de todas las partes interesadas en la gestión de riesgos, promoviendo el monitoreo, seguimiento y revisión en cada una de sus etapas. Lo anterior con el propósito de garantizar el cumplimiento de los planes de tratamiento y monitoreo periódico de controles existentes, la implementación efectiva de los controles y acciones definidos, y el desarrollo de procesos de control y gestión que aseguren la efectividad de las medidas adoptadas y el logro de los objetivos institucionales. Estas responsabilidades se encuentran alineadas con la línea estratégica institucional y con el enfoque de las tres líneas de defensa del Modelo Integrado de Planeación y Gestión (MIPG), a través del cual se establecen directrices para la gestión del riesgo, así como los mecanismos de revisión, retroalimentación y mejora continua de las políticas y controles implementados en la Entidad.

3.2 Metodología

Con la gestión del riesgo se busca fortalecer las medidas de prevención y control de las actividades desarrolladas en el ICBF para los Riesgos de Seguridad y Privacidad de la Información, Ciberseguridad, y Continuidad de la Operación, a partir de la identificación de riesgos de activos de información priorizados, análisis, valoración, manejo (tratamiento del riesgo), monitoreo de controles existentes de los riesgos, así como la evaluación del riesgo residual.

Para la Gestión de Riesgos de Seguridad y Privacidad de la información, Ciberseguridad y Continuidad de la Operación en el ICBF se contemplan las siguientes fases:

Figura 1: Metodología de Gestión de Riesgos



Para la Gestión de Riesgos de Seguridad y Privacidad de la Información, Ciberseguridad, y Continuidad de la Operación, como primera medida se establecen los siguientes roles:

- **Gestor de Riesgos de Seguridad de la Información:** es el responsable de dirigir, coordinar y realizar seguimiento a la gestión de riesgos de seguridad de la información en sus fases de establecimiento del alcance, contexto y criterios del proceso, análisis, identificación, valoración, monitoreo, tratamiento y evaluación del riesgo residual para los diferentes niveles.

- **Promotor EPICO:** apoya la sostenibilidad y mejoramiento continuo del sistema integrado de gestión y es el responsable de coordinar la identificación y realizar seguimiento a la gestión de riesgos en los procesos de la Sede de la Dirección General, reportando los soportes o evidencias de cumplimiento de las actividades de los planes de tratamiento y seguimiento a controles existentes al Gestor de Riesgos de Seguridad de la Información.

- **Referente SIGE:** apoya la sostenibilidad y mejoramiento continuo del sistema integrado de gestión y es el responsable de coordinar la identificación y realizar seguimiento a la gestión de riesgos en las regionales, reportando los soportes de cumplimiento de las actividades de los planes de tratamiento al Gestor de Riesgos de Seguridad de la Información.

- **Dueño del Riesgo:** es responsable de contribuir con el seguimiento y control a la gestión de los riesgos identificados (aceptación de riesgos inherentes y residuales) además de la aprobación de los controles existentes y los definidos en la fase de tratamiento. Para los procesos de la SDG el dueño del riesgo es el líder o responsable del proceso, para las regionales son los directores de las regionales.

3.2.1 Identificación de Riesgos de Activos de Información Priorizados

3.2.1.1 Establecimiento del Alcance, Contexto y Criterios

El Instituto Colombiano de Bienestar Familiar – ICBF, es un establecimiento público, es decir, es una entidad dotada de personería jurídica, autonomía administrativa y patrimonio propio; creada mediante la Ley 75 de 1968, es la entidad del Estado Colombiano con casi medio siglo de experiencia en la protección integral de los niños, niñas, adolescentes, y de acuerdo con la nueva estructura de la entidad, desde el 2020 el ICBF fortalece las capacidades de los jóvenes y las familias como actores clave de los entornos protectores y principales agentes de transformación social. El ICBF brinda atención a niños, niñas, adolescentes, jóvenes y familias, especialmente a aquellos en condiciones de amenaza, inobservancia o vulneración de sus derechos. Desde el año 2011 se encontraba adscrito al Sector de la Inclusión Social y la Reconciliación, y a partir de junio de 2023, mediante el Decreto 1074, fue adscrito al Sector Administrativo de Igualdad y Equidad, en

cabeza del Ministerio de Igualdad y Equidad. El Instituto cuenta con 33 regionales, ubicadas en los Departamentos y en el Distrito Capital y 216 Centros Zonales que hacen presencia en el ámbito municipal y local en todo el territorio nacional; llegando a más de ocho (8) millones de colombianos con el servicio público de bienestar familiar, a través de sus programas y estrategias de atención

3.2.2 Identificación y Valoración de Riesgos

Como paso inicial para la identificación de Riesgos de Seguridad y Privacidad de la Información, Ciberseguridad, y Continuidad de la Operación, se debe validar cuales son los activos priorizados del inventario de activos de información. Así mismo, se deben evaluar los diferentes aspectos de la entidad como infraestructura física, infraestructura tecnológica, procesos institucionales, entorno y demás factores internos y externos que puedan influir en la operación. Este análisis integral permite reconocer las situaciones potenciales que podrían generar afectaciones a la Entidad, comprometer los activos de información o poner en riesgo el cumplimiento de los objetivos institucionales.

- **Identificación de Riesgos de Activos de Información Priorizados:** Se denomina activo de información aquello que representa valor para la organización y por lo tanto debe protegerse con el propósito de mantener la Integridad, Confidencialidad y Disponibilidad de la información en el marco del modelo de operación por procesos. mediante la identificación y formalización de un inventario de activos de información, el Instituto Colombiano de Bienestar Familiar – ICBF reconoce cuáles son los activos de información críticos para la entidad según los lineamientos establecidos en la Guía para el desarrollo de inventario y clasificación de activos G10.GTI.

Seguido de la identificación, se debe tener en cuenta las siguientes características:

- Estar en términos cualitativos.
- Debe Incluir las causas y vulnerabilidades.
- Se debe indicar qué principio(s) es(son) afectado(s) (Confidencialidad, Integridad, Disponibilidad).

Una vez validados los activos priorizados se deberá asociar a un riesgo de acuerdo con el principio afectado (confidencialidad, integridad y disponibilidad), conforme a la guía de levantamiento de activos de información y la siguiente clasificación:

- **Riesgos de Seguridad de la Información**: posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento

y sus consecuencias[1] que afecta la confidencialidad, integridad o disponibilidad de la información.

- **Riesgos de Ciberseguridad:** son amenazas y vulnerabilidades que pueden comprometer la seguridad de los sistemas de información y los datos en el entorno digital. A continuación, se anuncian algunos ejemplos: Ransomware, malware, ataques de denegación de servicios (DDoS), ataque de hombre en el medio entre otros

- **Riesgos Emergentes**: son aquellos que se originan por la adopción, uso, integración o dependencia de tecnologías que aún se encuentran en proceso de maduración, estandarización o adopción generalizada. Estas tecnologías suelen evolucionar rápidamente y, debido a su novedad, presentan incertidumbres, vacíos normativos, limitada experiencia operativa y amenazas aún no completamente identificadas.

- **Riesgos de Continuidad de la Operación:** corresponden a aquellas situaciones que pueden generar indisponibilidad, interrupciones o afectaciones en los recursos esenciales que soportan los servicios críticos de la Entidad, incluyendo personas, infraestructura física, proveedores, información, sistemas y plataformas tecnológicas. Estos riesgos pueden comprometer la capacidad del ICBF para mantener la prestación oportuna y efectiva de sus servicios misionales, especialmente ante eventos inesperados o fallas técnicas.

  A continuación, se presentan algunos ejemplos de escenarios que pueden originar riesgos asociados a la continuidad de la operación:

  a. Fallo en el fluido eléctrico, que afecte los servicios, equipos o instalaciones esenciales.
  b. Interrupción en los canales de comunicaciones, incluyendo enlaces de datos, servicios de Internet o redes WAN.
  c. Falla física en los servidores de almacenamiento, que comprometa el acceso a datos o sistemas críticos
  d. Daños o fallos en el centro de cableado, afectando la infraestructura de red interna o la distribución de conectividad.
  e. Daños o fallos en el centro de cableado, afectando la infraestructura de red interna o la distribución de conectividad.
  f. Interrupciones en los medios de conexión entre centros de cableado o nodos de red, generando pérdida parcial o total de conectividad interna.

[1] Tomado de (ISO/IEC 27000)

3.2.3 Análisis de Riesgos

El análisis de los riesgos se inicia a partir de los activos de información priorizados, identificando las actividades, procesos y recursos asociados que, en función de las amenazas y vulnerabilidades presentes, podrían generar la materialización de riesgos de seguridad de la información. Este análisis permite comprender cómo un evento de riesgo puede afectar la operación institucional y establecer las condiciones bajo las cuales se produce dicha afectación. Posteriormente, se evalúa el impacto potencial del riesgo sobre la Entidad, considerando dos dimensiones principales: reputacional y económica, sin tener en cuenta los controles existentes, con el fin de determinar el nivel de riesgo inherente, conforme a las mejores prácticas internacionales en gestión del riesgo.

Para la estimación de la probabilidad, se deben considerar datos que permitan fundamentar el análisis de manera objetiva, tales como:

- **Datos internos:** incidentes históricos relacionados con el riesgo, información derivada del sistema de gestión de incidentes, reportes internos, tendencias evidenciadas y el conocimiento especializado del dueño del riesgo.
- **Datos externos:** información oficial emitida por entidades regulatorias o competentes, estudios sectoriales, reportes de ciberseguridad, boletines del CSIRT, estadísticas de riesgos similares en el entorno, y cualquier dato que permita contextualizar la probabilidad desde un enfoque externo.

3.2.4 Valoración del Riesgo

En esta fase se identifican, analizan y documentan los controles existentes que contribuyen a la mitigación del riesgo, relacionando aquellos que permiten disminuir su probabilidad de ocurrencia o limitar el impacto en caso de materialización. Cada control debe estar claramente asociado con las amenazas y vulnerabilidades previamente identificadas, garantizando que su diseño y propósito respondan de manera efectiva a los factores que originan el riesgo.
A partir de esta información, se deben determinar los controles adicionales necesarios para complementar o fortalecer los existentes, y evaluar cómo su implementación modifica los niveles de probabilidad e impacto. Este proceso permite establecer el nivel de **riesgo residual**.
La valoración debe incluir un **análisis de costo-beneficio**, mediante el cual se evalúe para cada control su diseño, implementación, efectividad y eficiencia, con el fin de determinar su pertinencia dentro del plan de tratamiento del riesgo. Este análisis orienta la toma de decisiones respecto a la priorización de controles y al tipo de tratamiento requerido, asegurando el uso adecuado de los recursos institucionales y el cumplimiento de los objetivos de seguridad de la información, ciberseguridad y continuidad de la operación.

3.2.5 Manejo del riesgo

El manejo del riesgo consiste en la selección y aplicación de la opción de tratamiento más adecuada, teniendo en cuenta el nivel de riesgo inherente, la naturaleza del activo afectado y las prioridades institucionales.

Los riesgos clasificados en nivel Bajo podrán ser aceptados por decisión del dueño del riesgo, siempre que:

- Los controles existentes se encuentren debidamente identificados e implementados,
- Los controles cubran de manera efectiva todas las causas asociadas al riesgo, y se mantenga un monitoreo periódico para garantizar que el nivel de riesgo no aumente.

Para los demás niveles de riesgo, y en coherencia con el nivel inherente obtenido durante el análisis, se deben considerar las siguientes opciones de tratamiento:

- **Mitigar:** es reducir la probabilidad de ocurrencia y/o el impacto del riesgo, mediante la implementación de controles, acciones o medidas.

- **Evitar el riesgo:** tomar las medidas encaminadas a prevenir su materialización, decidir no iniciar o continuar la actividad que lo originó.

- **Compartir o transferir el riesgo:** reduce su efecto compartiéndolo con una o varios de los procesos o partes (incluyendo los contratos y la financiación del riesgo).

- **Aceptar el riesgo:** decisión que toma el dueño del riesgo de aceptar las consecuencias y probabilidad de un riesgo en particular, retener el riesgo mediante una decisión informada. Esta opción solo puede aplicarse para los riesgos que se encuentren en el nivel bajo que tengan identificados los controles existentes que se tienen implementados para que estén en ese nivel y que a su vez abarquen todas las causas.

Para la definición de los planes de tratamiento es necesario tener en cuenta lo siguiente:

- Control del Sistema de Gestión de Seguridad de la Información: Corresponde al nombre del control o conjunto de controles establecidos en el Anexo A de la ISO/IEC 27001:2022. Cada control seleccionado debe estar directamente relacionado con las actividades propuestas en el plan de tratamiento, garantizando coherencia entre la causa del riesgo, las vulnerabilidades identificadas y la medida de control aplicada. Estos controles permiten orientar la implementación de acciones preventivas, detectives, correctivas o de mejora, y deben alinearse con el nivel de riesgo, los objetivos del SGSI y las necesidades de protección de los activos de información de la Entidad. Los riesgos

-

- **Actividades:** las actividades propuestas para el tratamiento deben impactar en la mitigación del riesgo (contrarrestar las vulnerabilidades y amenazas, principalmente las que no tienen un control asociado). Igualmente, debe estar relacionado con el control descrito en la opción “Nombre del control”. Su descripción debe iniciar con un verbo en infinitivo y establecer cómo se realiza, fecha de inicio, fecha de terminación y la evidencia del cumplimiento.

- **Responsable:** para cada actividad de tratamiento se debe definir el responsable de su ejecución. Para el caso del sistema de información se registrará como responsable al Promotor EPICO o Ingeniero Regional como responsable del cargue de la evidencia.

3.2.6 Monitoreo

El Gestor de Riesgos de Seguridad de la Información realizará seguimiento y revisión del cumplimiento de los controles existentes, planes de tratamiento, así como la recolección y verificación de las evidencias de cada una de las actividades realizadas.

Así mismo, los planes de tratamiento serán evaluados periódicamente para determinar el estado en el que se encuentra mediante el sistema de información.

Por lo anterior previamente a la valoración del riesgo residual de forma periódica, los Promotores EPICO o Referentes del Seguridad de las Regionales monitorearán y evaluarán el cumplimiento de los controles implementados en el sistema de información. Lo anterior, para determinar si son efectivos, moderadamente efectivos o poco efectivos, realizando los respectivos reportes al Gestor de Riesgos de Seguridad de la Información a través de la aplicación SVE, anexando las evidencias de cumplimiento, conforme a la programación establecida por dicho Gestor para la vigencia.
El monitoreo se realizará para todos los riesgos identificados (bajo, moderado, alto y extremo) y en este se deberá indicar también si se ha materializado o no el riesgo.

3.2.7 Evaluación del riesgo residual

Una vez finalizado los planes de tratamiento, se procede a realizar la evaluación del nivel residual. Para dicha evaluación nuevamente se determinará a partir de la aplicación de los controles y desarrollo de las actividades de los planes de tratamiento de riesgos, la probabilidad y el impacto. Esta evaluación debe estar soportada por un acta donde se especifique la evaluación del riesgo residual, la cual deberá ser firmada por el dueño o responsable del riesgo y las personas que participaron en la evaluación.

3.2.7.1 Nivel Inherente VS Nivel Residual

La calificación del riesgo de esta fase será el insumo para iniciar la identificación de riesgos para la siguiente vigencia.

- Si el resultado de la evaluación del nivel residual es menor a la inherente, se concluye que sus controles fueron adecuados y se pueden seguir implementando.

- Si el resultado de la evaluación del nivel residual es igual o superior a la evaluación inherente, se concluye que los controles no fueron adecuados por lo tanto se debe plantear un nuevo plan de tratamiento hasta que el riesgo pueda mitigarse.

3.2.8 Oportunidad de Mejora

Las oportunidades de mejora identificadas durante el proceso de gestión de riesgos, ya sea en la valoración inherente, la ejecución de los planes de tratamiento, el monitoreo de controles o la evaluación del riesgo residual, deberán ser documentadas y analizadas con el fin de fortalecer la eficacia del Sistema de Gestión de Seguridad de la Información. Estas oportunidades podrán originarse por necesidades de actualización de controles, ajustes metodológicos, cambios tecnológicos, variaciones en el contexto institucional o hallazgos derivados de auditorías internas o externas. El Gestor de Riesgos de Seguridad de la Información será responsable de consolidar dichas oportunidades, priorizarlas y coordinar las acciones requeridas para su implementación y registro en el aplicativo SVE, con el propósito de contribuir a la mejora continua del proceso de gestión de riesgos y del Sistema de Gestión de Seguridad de la Información.

3.2.9 Materialización

En caso de materializarse un riesgo, este deberá ser reportado conforme al Procedimiento de Gestión de Incidentes de Seguridad, Privacidad de la Información o Ciberseguridad. En el sistema de información se deberán identificar y registrar las actividades realizadas, considerando los factores internos o externos que contribuyeron a su ocurrencia.

Posteriormente, se deberá analizar el riesgo materializado, evaluar la efectividad de los controles existentes y determinar el nuevo nivel de riesgo posterior al incidente, registrando los ajustes correspondientes en el sistema de información SVE. Así mismo, será necesario evaluar el plan de tratamiento asociado y definir si requiere ajustes o la elaboración de un nuevo plan.
Si el incidente de seguridad no cuenta con un riesgo previamente asociado, se deberá analizarlo, identificarlo y valorarlo. En los casos en que se materialice un riesgo relacionado con tecnologías emergentes, deberá aplicarse la tipificación definida para este tipo de riesgos y realizar su correspondiente identificación y valoración.

Todo nuevo riesgo identificado, derivado o no del incidente materializado, deberá ser reportado al Director(a) de la Dirección de Tecnologías de la Información, con copia al Gestor de Riesgos de Seguridad de la Información, para que se inicie su registro y análisis formal dentro del sistema.

3.2.10. Recursos

El Instituto Colombiano de Bienestar Familiar ICBF en el marco de la Riesgos de Seguridad y Privacidad de la Información, Ciberseguridad, y Continuidad de la Operación, dispone de los siguientes recursos:

Recursos	Variable
Humanos	La Dirección de Tecnologías de la Información a través del Eje de seguridad de la Información es responsable de coordinar, implementar, modificar y realizar seguimiento a las políticas, estrategias y procedimientos en la Entidad en lo concerniente a la seguridad y privacidad de la información lo cual contribuye a la mejora continua.
Técnicos	- Guía de Gestión de Riesgos y Peligros - Plataforma SVE para la gestión de riesgos.
Logísticos	Gestión de recursos para realizar socializaciones, transferencia de conocimientos y seguimiento a la gestión de riesgos.
Financieros	Recursos destinados para la adquisición de conocimiento, recursos técnicos, así como aquellos requerido para la vinculación de recursos humanos y el desarrollo de auditorías.

3.2.11. Tiempo de Ejecución – Plan de Trabajo

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, Ciberseguridad y Continuidad de la Operación se actualiza y aprueba anualmente. Su seguimiento se desarrolla conforme a lo establecido en el plan de trabajo, el cual se ejecuta en la Sede de la Dirección General, las Direcciones Regionales y los Centros Zonales. Dicho seguimiento permite verificar el avance, cumplimiento y efectividad de las acciones definidas para la mitigación de los riesgos identificados.

Actividades	Tareas	Responsable de la Tarea	Entregable	Programación Tareas		
				Fecha inicio	Fecha final	Mes Cumplimiento
1. Socializar la Guía de Gestión de Riesgos y Peligros en lo relacionado con la Gestión de Riesgos de	1.1. Dar a conocer la Guía de Gestión de Riesgos y Peligros en la SDG y Regionales.	Profesional de la Dirección de Tecnologías de la Información, encargado de la	Formato de listado de asistencia o Listado de Asistencia de	02/02/2026	30/03/2026	

Actividades	Tareas	Responsable de la Tarea	Entregable	Programación Tareas		
				Fecha inicio	Fecha final	Mes Cumplimiento
Seguridad y Privacidad de la Información, Ciberseguridad, y Continuidad de la Operación		Gestión de Riesgos de Seguridad de la Información.	Microsoft Teams o Listados de asistencia por Microsoft Forms o Grabación de la sesión. Presentación realizada en las sesiones			Marzo
2. Identificar, analizar y valorar los Riesgos de Seguridad y Privacidad de la Información, Ciberseguridad y continuidad de la Operación	2.1. Gestionar con los procesos y regionales la Identificación, Análisis, valoración y definición del manejo de los Riesgos de Seguridad y Privacidad de la Información, Ciberseguridad, y Continuidad de la Operación	Profesional de la Dirección de Tecnologías de la Información, encargado de la gestión de Riesgos de Seguridad de la Información. Promotores EPICO de la SDG Ingenieros Regionales	Actas de identificación de riesgos - Información registrada en SVE	02/02/2026	30/04/2026	Abril
	2.2. Realizar la retroalimentación, revisión y verificación de los riesgos identificados por la SDG y Regionales, validando la definición de los planes de tratamiento y controles existentes	Profesional de la Dirección de Tecnologías de la Información, encargado de la gestión de Riesgos de Seguridad de la Información.	Correos electrónicos con el Plan Operativo SGSI	02/02/2026	30/04/2026	Abril
3. Realizar seguimiento Fase de manejo y monitoreo de los Riesgos de Seguridad y Privacidad de la Información, Ciberseguridad, y Continuidad de la Operación	3.1. Definir el cronograma para el seguimiento de los planes de tratamiento y monitoreo a controles existentes.	Profesional de la Dirección de Tecnologías de la Información, encargado de la gestión de Riesgos de Seguridad de la Información.	Correo de la Subdirección de mejoramiento donde remite el plan operativo SGSI aprobado	02/02/2026	17/04/2026	Abril
	3.2. Realizar seguimiento a los riesgos identificados en la SDG y Regionales con sus planes de tratamiento y monitoreo de controles existentes.	Profesional de la Dirección de Tecnologías de la Información, encargado de la gestión de Riesgos de Seguridad de la Información. Promotores EPICO de la SDG Ingenieros Regionales	Correo mensual con la Calificación del Plan Operativo para la Gestión de Riesgos – Actas y memorandos de identificación de Riesgos	30/04/2026	18/12/2026	Diciembre

Actividades	Tareas	Responsable de la Tarea	Entregable	Programación Tareas		
				Fecha inicio	Fecha final	Mes Cumplimiento
4. Realizar la evaluación de riesgos residuales	4.1. Realizar acompañamiento en la evaluación de riesgos residuales en la SDG y Regionales.	Gestor de riesgos SGSI, Profesional EPICO Referente SGSI - Ingeniero Regional	Acta de evaluación de Riesgo Residual	30/04/2026	18/12/2026	Diciembre
5. Revisar la Guía Gestión de Riesgos y Peligros en lo relacionado con los Riesgos de Seguridad y Privacidad de la Información, Ciberseguridad, y Continuidad de la Operación	5.1. Revisar la Guía Gestión de Riesgos Seguridad de la Información y en caso de que se requiera gestionar su actualización.	Profesional de la Dirección de Tecnologías de la Información, encargado de la gestión de Riesgos de Seguridad de la Información.	Guía Gestión de Riesgos y Peligro Actualizada o Correo en el cual se indique que no es necesario la actualización	03/11/2026	31/12/2026	Diciembre
6. Fortalecer la Gestión de Proyectos de TI de los Riesgos de Seguridad y Privacidad de la Información, Ciberseguridad, y Continuidad de la Operación	6.1. Realizar seguimiento y monitoreo a los Riesgos de TI identificados por el Proveedor de Servicios Tecnológicos	Profesional de la Dirección de Tecnologías de la Información, encargado de la gestión de Riesgos de Seguridad de la Información. Profesional de la Dirección de Tecnologías de la Información, encargados de construir los proyectos de TI.	Actas de reunión o Formato de listado de asistencia o Listado de Asistencia de Microsoft Teams o Listados de asistencia por Microsoft Forms o Grabación de la sesión o Correos electrónicos cuando aplique o informes de Gestión	01/02/2026	30/06/2026	Junio
7. Materialización	Consolidar los reportes de materialización de riesgos y/o de incidentes que afecten la seguridad y privacidad de la información de la Entidad	Profesional de la Dirección de Tecnologías de la Información, encargado de la gestión de Riesgos de Seguridad de la Información. Ingenieros Regionales	Informe cuatrimestral de la Gestión de riesgos	08/05/2026	31/12/2026	Diciembre
8. Monitoreo y Revisión	Reporte de Indicador PA-142	Profesional de la Dirección de Tecnologías de la Información, encargado de la gestión de Riesgos de Seguridad de la Información. Ingenieros Regionales	Correo Electronico Reporte de Indicador PA-142	08/05/2026	31/12/2026	Diciembre

3.2.12. Presupuesto

La estimación y asignación del presupuesto para el plan de tratamiento de Riesgos de Seguridad y Privacidad de la Información, Ciberseguridad, y Continuidad de la Operación identificados en la entidad, corresponderá al dueño del riesgo, quien es el responsable de contribuir con el seguimiento y control de la gestión, además de la implementación de los controles definidos en el plan de tratamiento.

3.2.13. Medición del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, Ciberseguridad, y Continuidad de la Operación

La medición se realiza con el indicador de gestión PA 142 “Porcentaje de cumplimiento de las actividades definidas en los planes de tratamiento de Riesgos de Seguridad y Privacidad de la Información, Ciberseguridad y Continuidad de la Operación” que está orientado principalmente a determinar el porcentaje de ejecución de actividades definidas en el tratamiento de riesgos de seguridad de la información ubicados en zonas extremo, alto y moderado.

4. DOCUMENTOS DE REFERENCIA

- Resolución 3248 del 2 de Julio de 2025 “Por la cual se adopta la Política de Seguridad y Privacidad de la Información, Ciberseguridad y Continuidad de la Operación”, o la norma que la modifique, sustituya o derogue.
- Resolución 11980 del 30 de diciembre de 2019 “Por la cual se adopta el modelo de Planeación y Sistema Integrado de Gestión del ICBF “.
- Resolución 6659 del 15 de diciembre de 2020 “Por la cual se modifica el modelo de Planeación y sistema Integrado de Gestión del ICBF “.
- Decreto 1430 del 24 de diciembre de 2025 “Por la cual se modifica la estructura del Instituto Colombiano de Bienestar Familiar Cecilia de la Fuente de Lleras“.
- Resolución No. 8650 de 2021 “Por la cual se integra y reglamenta el Comité Institucional de Gestión y Desempeño, el Subcomité de Arquitectura Empresarial y Mesa Técnica de Sistemas y Gestión de Información misional en el Instituto Colombia de Bienestar Familiar”
- Guía para la administración del riesgo y el diseño de controles en entidades públicas. Versión 5. Departamento Administrativo para la Función Pública (DAFP) año 2020
- G3.MI Guía de Gestión de Riesgos y Peligros
- Ley 23 de 1982 sobre derechos de autor
- Ley 44 de 1993 “Por la cual se modifica y adiciona la Ley 23 de 2082 y se modifica la Ley 29 de 2044 y Decisión Andina 351 de 2015 (Derechos de autor)
- Ley 527 de 1999 “Por 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”

- Ley 594 de 2000 “Por medio de la cual se expide la Ley General de Archivos”
- Ley 1266 de 2008 “Por la cual se dictan las disposiciones generales del Habeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones”
- Ley 1221 del 2008 “Por la cual se establecen normas para promover y regular el teletrabajo y se dictan otras disposiciones”
- Ley 1273 de 2009 “Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones”
- Ley 1581 de 2012 “Por la cual se dictan disposiciones generales para la protección de datos personales”
- Ley 1712 de 2014 “Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones”
- Ley 1753 de 2015 “Por la cual se expide el Plan Nacional de Desarrollo 2014-2018 “Todos por un nuevo país”.
- Ley 1755 de 2015 “Por medio de la cual se regula el Derecho Fundamental de Petición y se sustituye un título del Código de Procedimiento Administrativo y de lo Contencioso Administrativo”
- Ley 2052 de 2020 “Por medio de la cual se expide el código general disciplinario”
- Ley 1915 de 2018 “Por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos”
- Ley 2088 de 2021 “Por la cual se regula el trabajo en casa y se dictan otras disposiciones.
- Ley 2108 de 2021 “Ley de Internet como servicio público esencial y universal” o por medio de la cual se modifica la Ley 1341 de 2009 y se dictan otras disposiciones”
- Decreto 886 de 2014 “Por el cual se reglamenta el Registro Nacional de Bases de Datos”
- Decreto 1074 de 2015 “Por medio del cual se expide el Decreto reglamentario del sector comercio, industria y turismo. Reglamenta parcialmente la Ley 1581 de 2012 e imparten instrucciones sobre el Registro Nacional de Bases de Datos. Artículos 25 y 26”
- Decreto 1078 de 2015 “Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones”
- Decreto 1081 de 2015 “Por medio del cual se expide el Decreto Reglamentario del Sector Presidencia”
- Decreto 612 de 2018 “Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado”
- Decreto 88 de 2022 “Por el cual se adiciona el Titulo 20 a la parte 2 del libro 2 del Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de establecer los lineamientos generales para fortalecer la

gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones.

- Decreto 338 de 2022 “Por el cual se adiciona el Titulo 21 a la parte 2 del libro 2 del Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones
- Decreto 767 de 2022 “Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones”
- Resolución 500 de 2021 “Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la Política de Gobierno Digital”
- Resolución 746 de 2022 “Por la cual se fortalece el Modelo de Seguridad y Privacidad de la Información y se definen lineamientos adicionales a los establecidos en la Resolución No. 500 de 2021”
- Resolución 02277 de 2025 “Por medio de la cual el Ministerio TIC actualiza el Modelo de Seguridad y Privacidad de la Información”
- Directiva Presidencial 03 de 2021 “Lineamientos para el uso de servicios en la nube, inteligencia artificial, seguridad digital y gestión de datos”
- Directiva Presidencial 02 de 2022 “Reiteración de la política pública en materia de seguridad digital”
- CONPES 3995 de 2020: Política Nacional de Confianza y Seguridad Digital”
- CONPES 4144 de 2025: Política Nacional de Inteligencia Artificial
- Norma ISO/IEC 27001:2022: Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de la seguridad de la información.
- ISO/IEC 27005:2022 Proporciona directrices para la gestión del riesgo de seguridad de la información
- Guía para la Gestión Integral del Riesgo en Entidades Públicas del Departamento Administrativo de la Función Pública (DAFP).

5. CONTROL DE CAMBIOS

Fecha	Versión	Descripción del Cambio
N/A	N/A	N/A