TABLA DE CONTENIDO

PÚBLICA

RESUMEN EJECUTIVO

Para el desarrollo del plan de tratamiento de riesgos el ICBF estableció la G3.MI (Guía de Riesgos y Peligros) la cual presenta los lineamientos para poder identificar, analizar, valorar, tratar, evaluar y monitorear los riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad del Negocio en la Sede de la Dirección General y las 33 regionales del ICBF.

El objetivo de este plan es definir y aplicar los lineamientos para tratar de manera integral los riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad del Negocio a los que el ICBF pueda estar expuesto. Preservar integridad, confidencialidad, disponibilidad y autenticidad de la información.

En el plan se define un cronograma de trabajo, en el cual se establecen las siguientes actividades:

- Dar a conocer la Guía y Herramienta - Gestión de Riesgos de Seguridad y privacidad de la Información, Seguridad Digital y Continuidad del Negocio en la SDG y Regionales.
- Brindar orientación en la Identificación, Análisis, valoración y definición del manejo de los Riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad del negocio tecnológica en la SDG y Regionales.
- Realizar la realimentación, revisión y verificación de los riesgos identificados con sus planes de tratamiento y controles existentes en la SDG y Regionales.
- Definir el cronograma para el seguimiento de los planes de tratamiento y controles existentes.
- Realizar seguimiento a los riesgos identificados en la SDG y Regionales con sus planes de tratamiento y controles existentes. Validar si se han materializado.
- Realizar acompañamiento en la evaluación de riesgos residuales en la SDG y Regionales.
- Actualizar la Guía Gestión de Riesgos Seguridad de la Información en caso de que se requiera.
- Monitorear y reportar el resultado del indicador PA 142 “Porcentaje de cumplimiento de las actividades definidas en los planes de tratamiento de riesgos de seguridad y privacidad de la información y seguridad digital”.

Como herramienta de seguimiento asociado a este plan se tiene el indicador PA 142 “Porcentaje de cumplimiento de las actividades definidas en los planes de tratamiento de riesgos de seguridad y privacidad de la información y seguridad digital” que se evalúa de forma cuatrimestral.

PÚBLICA

INTRODUCCIÓN

La gestión de riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad del Negocio, le permite al ICBF realizar la identificación, análisis y tratamiento a los riesgos que pueden comprometer el cumplimiento de los objetivos trazados a favor de la niñez la adolescencia la juventud y las familias colombianas, contribuyendo en la toma de decisiones con el fin de prevenir la materialización de estos.

De acuerdo con lo mencionado, el ICBF ha tomado como referencia la normativa establecida por el estado colombiano, CONPES 3854 de 2016 y 3995 de 2020, Modelo de Seguridad y Privacidad del Ministerio de Tecnologías de la Información y lo establecido en el decreto 1008 de 14 de junio 2018, adoptando las buenas prácticas y los lineamientos establecidos en los estándares ISO 27001:2013, ISO 31000:2018, la guía para la administración del riesgo (DAFP) y políticas propias de la Entidad.

1. OBJETIVO GENERAL

Definir y aplicar los lineamientos para tratar de manera integral los riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad del Negocio a los que el Instituto Colombiano de Bienestar Familiar pueda estar expuesto; contribuyendo a que se alcancen los objetivos, la misión y la visión institucional; protegiendo y preservando la integridad, confidencialidad, disponibilidad y autenticidad de la información.

1.1 Objetivos Específicos

- Cumplir con los requisitos legales y reglamentarios pertinentes a la legislación colombiana respecto a los riegos de seguridad y privacidad de la información, seguridad de digital y Continuidad del Negocio.
- Identificar y dar tratamiento a los riesgos de Seguridad y Privacidad de la información, Seguridad Digital y Continuidad del Negocio de acuerdo con la metodología establecida por la entidad.
- Fortalecer y apropiar el conocimiento de los colaboradores referente a la gestión de riesgos Seguridad y Privacidad de la información, Seguridad Digital y Continuidad del Negocio.

2. ALCANCE

La gestión de riesgos de seguridad y privacidad de la información, seguridad digital y continuidad del Negocio aplica en la Sede de la Dirección General y las 33 regionales del ICBF.

PÚBLICA

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, tratar, evaluar y monitorear los riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad del Negocio en 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 pueden ser asumidos o aceptados a decisión del líder del proceso, y se deben identificar los controles que se tienen implementados para que estén en ese nivel.

Así mismo, se deben monitorear a través de la gestión de incidentes de seguridad de la información con el fin de realizar seguimiento a sus posibles materializaciones que puedan cambiar su nivel.

Para la ejecución del plan de tratamiento de riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad del Negocio, se realizarán las actividades acordes a lo establecido en el Plan de Seguridad y Privacidad de la Información.

3.1. Responsabilidades

El ICBF deberá definir los roles y responsabilidades de todas las partes interesadas en lo concerniente a la gestión de riesgos, promoviendo el monitoreo y revisión a la gestión en sus etapas con el propósito de dar cumplimiento a los planes de tratamiento proyectados, ejecutando los controles y acciones definidos, desarrollando e implementado procesos de control y gestión con el propósito de asegurar la efectividad y el cumplimiento de los objetivos institucionales.

Dichas responsabilidades son acordes a línea estratégica y las tres líneas de defensa del Modelo Integrado de Planeación y Gestión (MIPG), donde se aprueban las directrices para la gestión del riesgo en la entidad y la revisión y/o mejora de las políticas establecidas.

PÚBLICA

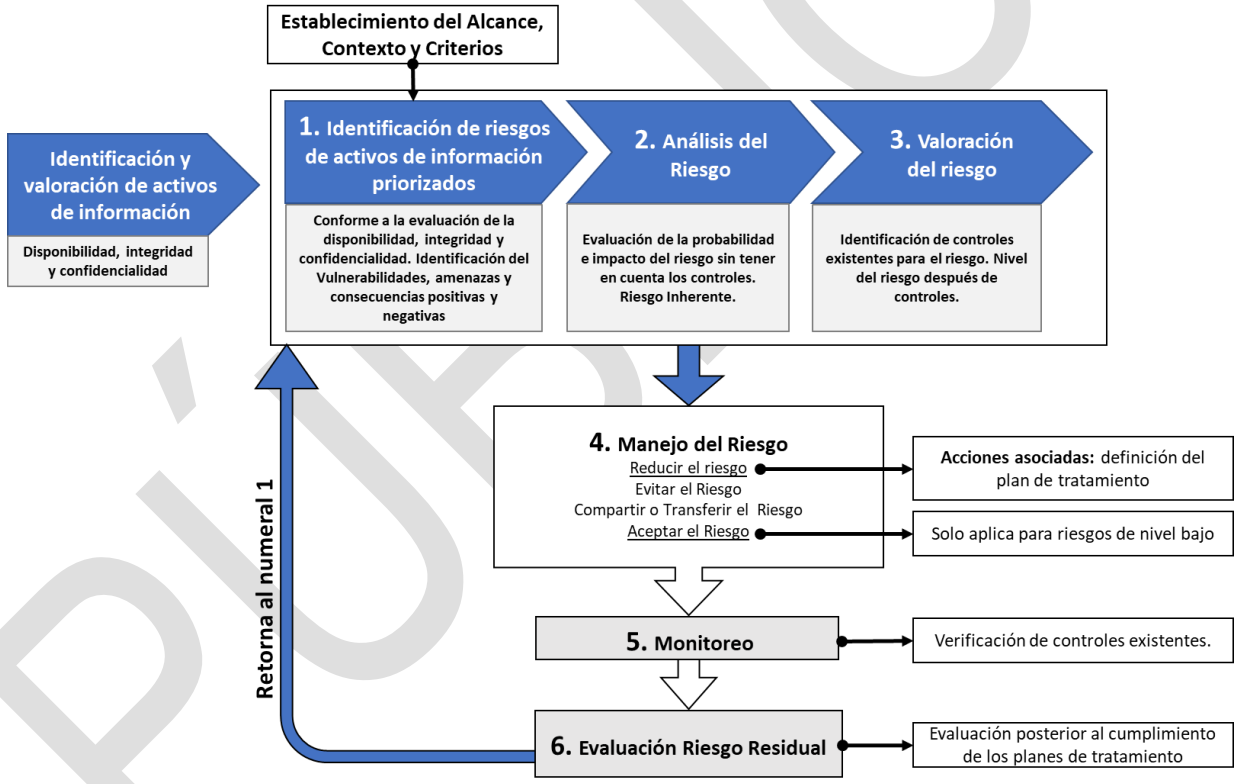
3.2 Metodología

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, Seguridad Digital y Continuidad del Negocio, a partir de la identificación de riesgos de activos de información priorizados, análisis, valoración, manejo (tratamiento del riesgo), monitoreo de los riesgos, así como la evaluación del riesgo residual.

.

Para la gestión de riesgos de Seguridad y Privacidad de la información, Seguridad Digital y Continuidad del Negocio 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, Seguridad Digital y Continuidad del Negocio, 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

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA.

sus fases de establecimiento del alcance, contexto y criterios del proceso, identificación, valoración, tratamiento y evaluación del riesgo residual para los diferentes niveles.

- **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, identificación, valoración, tratamiento y evaluación del riesgo residual para los diferentes niveles. En el sistema de información corresponderá al rol de administrador de riesgos de seguridad de la información.

- **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 de cumplimiento de las actividades de los planes de tratamiento al Gestor de Riesgos de Seguridad de la Información. En el sistema de información corresponderá al campo gestor de riesgos.

- **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. En el sistema de información corresponderá al campo gestor de riesgos.

- **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 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. En el sistema de información corresponderá al responsable del riesgo.

3.2.1. Identificación de Riesgos de Activos de Información Priorizados

3.2.1.1. Establecimiento del Alcance, Contexto y Criterios

El contexto interno del Instituto Colombiano de Bienestar Familiar ICBF se abordará desde un enfoque centrado en los aspectos que impactan directamente el desarrollo y la protección integral de la primera infancia, la niñez, la adolescencia, la juventud y el bienestar de las familias y comunidades colombianas. En este sentido se presentará la orientación estratégica, táctica y operativa que posibilita su actuar en el territorio como la Institución con casi medio siglo de

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA.

PÚBLICA

experiencia en la protección integral de la niñez en Colombia y como ente rector del Sistema Nacional de Bienestar Familiar.

El contexto externo del Instituto Colombiano de Bienestar Familiar – ICBF como institución pública posee una competencia única como ente rector del Sistema Nacional de Bienestar Familiar, frente al ejercicio de la Protección Integral de los niños, niñas y adolescentes, jóvenes y promueve el fortalecimiento familiar en Colombia; está configurado por un alto nivel de dinamismo y complejidad determinado por los aspectos sociales, legales, económicos, políticos, medioambientales y tecnológicos en la sociedad de la información.

3.2.2. Identificación y Valoración de Riesgos

Como paso inicial para la identificación de riesgos de seguridad de la información, seguridad digital y continuidad del negocio, 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, áreas de trabajo, entorno y ambiente en general y reconocer las situaciones potenciales que causarían daño a la entidad poniendo en riesgo el logro de sus objetivos.

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:

PÚBLICA

- **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 Seguridad Digital**: es la expresión usada para describir una categoría de riesgo relacionada con el desarrollo de cualquier actividad en el entorno digital. Este riesgo puede resultar de la combinación de amenazas y vulnerabilidades en el ambiente digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. El riesgo de seguridad digital es de naturaleza dinámica, incluye aspectos relacionados con el ambiente físico y digital, las personas involucradas en las actividades y los procesos organizacionales que las soportan[2].

- **Riesgos de Continuidad del Negocio**: son aquellos riesgos que involucran alguna afectación de la infraestructura tecnológica que soporta los servicios que brinda la Dirección de Información y Tecnología a la entidad, están asociados con la pérdida de disponibilidad.

3.2.3. Análisis de Riesgos

El análisis de los riesgos parte de los activos de información priorizados, asociando las actividades que dependiendo de las amenazas y vulnerabilidades pueden llegar a materializar riesgos de seguridad de la información. Finalmente, con esto se evalúa el impacto que tendría un riesgo sobre la entidad a partir de dos perspectivas: reputacional o económica. Lo anterior, debe realizarse sin tener en cuenta los controles existentes.

Los datos estadísticos que pueden servir como base para valorar la probabilidad pueden ser:

- Datos Internos (incidentes presentados con el riesgo o experticia y/o conocimiento del dueño del riesgo).

- Datos Externos (datos oficiales reportados por entes regulatorios y competentes que se relacionen con riesgos que afecten el contexto externo).

[1] Tomado de (ISO/IEC 27000)
[2] Tomado de Documento CONPES 3854 Política Nacional de Seguridad Digital

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA.

PÚBLICA

3.2.4. Valoración del Riesgo

En esta fase se realiza la identificación de controles existentes para la mitigación del riesgo, asociando todos los que contribuyan a reducir la probabilidad o controlar el impacto en caso de que llegue a materializarse. Igualmente, cada control debe relacionarse a las vulnerabilidades o amenazas que se identificaron para el riesgo, es decir se deben mitigar.

Por lo anterior se deben determinar los controles y verificar los cambios en las probabilidades e impactos de acuerdo con su aplicación y realizar un análisis de costo beneficio de cada uno de los controles evaluando para cada uno la ejecución y el diseño.

3.2.5. Manejo del riesgo.

Se puede aceptar el riesgo a decisión del líder del proceso para aquellos que estén en nivel bajo y se deben identificar los controles implementados para su mitigación. Los riesgos de nivel bajo se deben monitorear a través de la gestión de incidentes de seguridad de la información, con el fin de realizar seguimiento a sus posibles materializaciones que puedan generar cambios en su nivel.

Teniendo en cuenta el nivel inherente se determinarán las siguientes opciones de tratamiento:

- **Reducir el riesgo:** tomar medidas encaminadas a disminuir tanto la probabilidad (medidas de prevención) como el impacto (medidas correctivas). Esta opción corresponde a la definición de los planes de tratamiento, las cuales en el sistema de información se relacionarán en la opción de acciones asociadas.

- **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.

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 controles descritos en el Anexo A de la ISO 27001/2013. Este debe estar

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA.

PÚBLICA

relacionado con las actividades a implementar en el plan de tratamiento.

- **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, 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 que este último realice 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 determinada la calificación de los controles implementados, 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

PÚBLICA

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.

Nivel Inherente VS Nivel Residual.

- 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.

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

3.2.8. Oportunidad de Mejora

El Instituto Colombiano de Bienestar Familiar no sólo se centra en los riesgos identificados, sino que este análisis o apreciación del riesgo sirve de base para implementar oportunidades de mejora. Por lo anterior, la oportunidad de mejora debe definirse conforme a las consecuencias positivas que se identificaron previamente y en los resultados obtenidos de la ejecución de los planes de tratamiento. Para esto se deberá registrar en la Suite Vision Empresarial y remitirse un correo electrónico al Gestor de Riesgos de Seguridad de la Información comunicando el código de la oportunidad de mejora con la que quedó en el sistema.

3.2.9. Materialización

En el caso que un riesgo se lleve a cabo, este debe ser reportado de acuerdo con el procedimiento de gestión de incidentes de seguridad de la información y en el sistema se deben identificar las actividades a seguir teniendo en cuenta, tanto factores internos o externos que pueden propiciar el riesgo. Así mismo, se deberá analizar el riesgo y validar en que queda posterior a la materialización, registrando los cambios respectivos en el sistema de información. En caso de que se materialice un riesgo que no esté identificado, deberá ser reportado al Director de Información y Tecnología con copia al Gestor de Riesgos de Seguridad de la Información para que se inicie su correspondiente identificación en el sistema.

3.2.9.1. Incidentes de Seguridad de la Información

Uno de los enfoques y objetivos del Plan de Seguridad y Privacidad de la Información es la gestión de incidentes, ya que la atención y mitigación de vulnerabilidades conocidas y no

PÚBLICA

conocidas son de vital importancia para identificar mejoras en los controles implementados o definir nuevas actividades que permitan proteger la confidencialidad, disponibilidad e integridad de los activos de información de la Entidad.

En el 2022 se presentaron y atendieron un total de 16 incidentes de seguridad de la información, los cuales se discriminan de la siguiente manera:

TIPO DE INCIDENTE	CANTIDAD	PORCENTAJE
Indisponibilidad del activo de información	3	18,8%
Borrado de información	3	18,8%
Robo de equipo	2	12,5%
Suplantación de identidad	2	12,5%
Toma de control de equipo usuario final	1	6,3%
Explotación de vulnerabilidad AZURE	1	6,3%
Phishing	1	6,3%
Apropiación	1	6,3%
Malware	1	6,3%
Reporte IP institucional lista negra	1	6,3%
TOTAL	**16**	

4. RECURSOS

El Instituto Colombiano de Bienestar Familiar ICBF en el marco de la gestión de riesgos de seguridad y Privacidad de la información, Seguridad Digital y Continuidad del Negocio, dispone de los siguientes recursos:

RECURSOS	VARIABLE
Humanos	La Dirección de Información y Tecnología 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. Herramienta 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.

5. TIEMPO DE EJECUCION – PLAN DE TRABAJO

El plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información se actualiza y aprueba anualmente, el seguimiento se realiza conforme a lo definido en el plan de trabajo que se muestra a continuación el cual se ejecuta en la Sede de la Dirección General, Regionales y Centros Zonales:

¿Antes de imprimir este documento… piense en el medio ambiente!

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA.

PUBLICA

Actividades	Tareas	Responsable de la Tarea	Entregable	Programación Tareas	
				Fecha inicio	Fecha final
1. Sensibilización	1.1. Dar a conocer la Guía y Herramienta - Gestión de Riesgos de Seguridad y privacidad de la Información, Seguridad Digital y Continuidad del Negocio en la SDG y Regionales	Profesional de la dirección de Información y Tecnología, encargado de la gestión de Riesgos de Seguridad de la Información. Profesional de la dirección de Información y Tecnología, encargado de la gestión de Cambio y Cultura.	Formato listado de asistencia o Listado de Asistencia de Microsoft Teams o Listados de asistencia por Microsoft Forms o Grabación de la sesión	01/02/2023	31/03/2023
2. Identificación, análisis, valoración de Riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y continuidad del Negocio	2.1. Brindar orientación en la Identificación, Análisis, valoración y definición del manejo de los Riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad del negocio tecnológica en la SDG y Regionales	Profesional de la dirección de Información y Tecnología, encargado de la gestión de Riesgos de Seguridad de la Información.	Actas de identificación de riesgos Información registrada en SVE	01/02/2023	31/03/2023
	2.2. Realizar la realimentación, revisión y verificación de los riesgos identificados con sus planes de tratamiento y controles existentes en la SDG y Regionales	Profesional de la dirección de Información y Tecnología, encargado de la gestión de Riesgos de Seguridad de la Información.	Correos electrónicos	1/03/2023	16/04/2023
3. Seguimiento Fase de manejo y monitoreo del riesgo	3.1. Definir el cronograma para el seguimiento de los planes de tratamiento y controles existentes.	Profesional de la dirección de Información y Tecnología, encargado de la gestión de Riesgos de Seguridad de la Información.	Correos electrónicos	1/03/2023	16/04/2023
	3.2. Realizar seguimiento a los riesgos identificados en la SDG y Regionales con sus planes de tratamiento y controles existentes. Validar si se han materializado.	Profesional de la dirección de Información y Tecnología, encargado de la gestión de Riesgos de Seguridad de la Información.	Correo mensual con la Calificación del Plan Operativo para la Gestión de Riesgos - Actas de identificación o revaluación de riesgos, en caso de que haya alguna materialización	31/03/2023	31/12/2023
4. 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	Formato 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	01/05/2023	23/12/2023

PÚBLICA

Actividades	Tareas	Responsable de la Tarea	Entregable	Programación Tareas	
				Fecha inicio	Fecha final
5. Revisión de la Guía Gestión de Riesgos Seguridad de la Información	5.1. Actualizar la Guía Gestión de Riesgos Seguridad de la Información en caso de que se requiera.	Profesional de la dirección de Información y Tecnología, 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	03/07/2023	29/12/2023
6. Monitoreo y Revisión	6.1. Monitorear y reportar el resultado del indicador PA 142 “Porcentaje de cumplimiento de las actividades definidas en los planes de tratamiento de riesgos de seguridad y privacidad de la información y seguridad digital”	Profesional de la dirección de Información y Tecnología, encargado de la gestión de Riesgos de Seguridad de la Información.	Correo con el Informe del reporte del indicador conforme a su periodicidad de medición	03/04/2023	29/12/2023

6. PRESUPUESTO

La estimación y asignación del presupuesto para el plan de tratamiento de riesgos de Seguridad y Privacidad de la Información 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.

7. MEDICIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

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 y seguridad digital” 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.

8. DOCUMENTOS DE REFERENCIA

G3.MI Guía de Gestión de Riesgos y Peligros

9. CONTROL DE CAMBIOS

Fecha	Versión	Descripción del Cambio
N.A.		

PÚBLICA