
 BIENESTAR FAMILIAR	<b>PROCESO MEJORA E INNOVACION</b>	PL3.MI	31/01/2022
	<b>PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>	Versión 1	Página 1 de 12

## TABLA DE CONTENIDO

<b>INTRODUCCIÓN</b> .....	2
<b>1. OBJETIVO GENERAL</b> .....	2
1.1 Objetivos Específicos.....	2
<b>2. ALCANCE</b> .....	2
<b>3. DESARROLLO</b> .....	3
3.1 Responsabilidades .....	3
3.2 Metodología.....	4
3.3 Establecimiento del alcance, contexto y criterios.....	5
3.4 Identificación y Valoración de Riesgos .....	6
3.4.1 Identificación de riesgos de activos de información priorizados .....	6
3.4.2 Análisis de Riesgos.....	7
3.4.3 Evaluación de Riesgos.....	7
3.5 Tratamiento de riesgos.....	7
3.6 Evaluación del riesgo residual.....	9
3.7 Oportunidad de Mejora.....	9
3.8 Materialización .....	9
<b>4. RECURSOS</b> .....	9
<b>5. TIEMPO DE EJECUCION – PLAN DE TRABAJO</b> .....	10
<b>6. PRESUPUESTO</b> .....	12
<b>7. MEDICIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b> .....	12
<b>8. DOCUMENTOS DE REFERENCIA</b> .....	12
<b>9. CONTROL DE CAMBIOS</b> .....	12

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

	<b>PROCESO MEJORA E INNOVACION</b>	PL3.MI	31/01/2022
	<b>PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>	Versión 1	Página 2 de 12

## 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 riesgos 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.

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

 BIENESTAR FAMILIAR	<b>PROCESO MEJORA E INNOVACION</b>	PL3.MI	31/01/2022
	<b>PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>	Versión 1	Página 3 de 12

### 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.

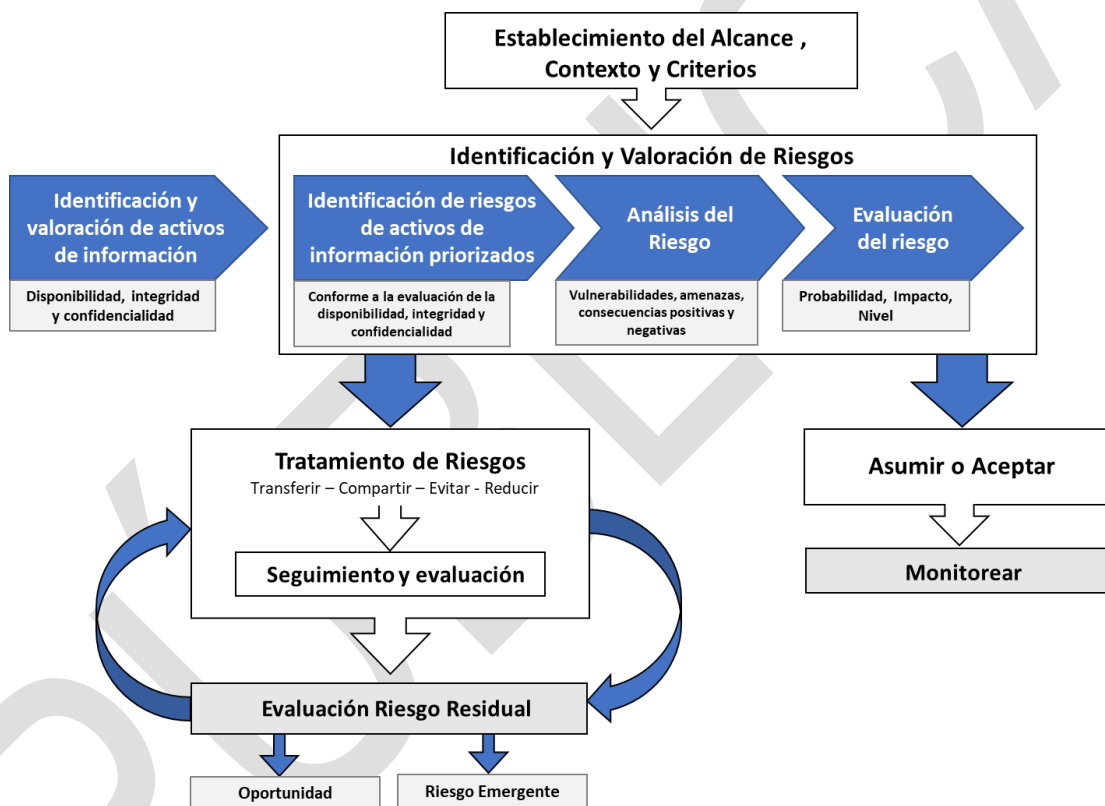
¿Antes de imprimir este documento... piense en el medio ambiente!

	<b>PROCESO MEJORA E INNOVACION</b>	PL3.MI	31/01/2022
	<b>PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>	Versión 1	Página 4 de 12

### 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, análisis, valoración y tratamiento de estos, conforme a lo establecido en la metodología definida por entidad, la cual se relaciona a continuación.


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

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

	<b>PROCESO MEJORA E INNOVACION</b>	PL3.MI	31/01/2022
	<b>PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>	Versión 1	Página 5 de 12


- **Profesional EPICO:** apoya la sostenibilidad y mejoramiento continuo del sistema integrado de gestión y es el responsable de coordinar la identificación de riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad del Negocio, así como de 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.
- **Referente SIGE:** apoya la sostenibilidad y mejoramiento continuo del sistema integrado de gestión y es el responsable de coordinar la identificación de riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad del Negocio, así como de 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 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.

### 3.3 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 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 que 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 que 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.

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

 BIENESTAR FAMILIAR	<b>PROCESO MEJORA E INNOVACION</b>	PL3.MI	31/01/2022
	<b>PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>	Versión 1	Página 6 de 12

### 3.4 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.

#### 3.4.1 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<sup>1</sup> 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

<sup>1</sup> Tomado de (ISO/IEC 27000)

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

	<b>PROCESO MEJORA E INNOVACION</b>	PL3.MI	31/01/2022
	<b>PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>	Versión 1	Página 7 de 12

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<sup>2</sup>.

- **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.

### 3.4.2 Análisis de Riesgos

El análisis de riesgos es un proceso cuantitativo y cualitativo donde se pretende determinar la probabilidad de ocurrencia de una eventualidad y el impacto que pueda causar la materialización del riesgo.

- La Probabilidad representa el número de veces que el riesgo se ha presentado o puede presentarse en un determinado tiempo.
- El impacto hace referencia a magnitud de sus efectos en caso de materialización.

### 3.4.3 Evaluación de Riesgos

La evaluación de riesgos pretende priorizar los riesgos identificados de acuerdo con el nivel inherente (criticidad) obtenido, evaluando y determinando la probabilidad, el impacto y controles existentes de acuerdo con las vulnerabilidades y amenazas identificadas.

## 3.5 Tratamiento de riesgos

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

- **Evitar el riesgo:** tomar las medidas encaminadas a prevenir su materialización, decidir no iniciar o continuar la actividad que lo originó.
- **Mitigar el riesgo:** tomar medidas encaminadas a disminuir tanto la probabilidad (medidas de prevención), como el impacto (medidas correctivas).

<sup>2</sup> Tomado de Documento CONPES 3854 Política Nacional de Seguridad Digital

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



**PROCESO  
MEJORA E INNOVACION**

PL3.MI

31/01/2022

**PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y  
PRIVACIDAD DE LA INFORMACIÓN**

Versión 1

Página 8 de  
12

- **Compartir el riesgo:** reduce su efecto compartiéndolo con una o varios de los procesos o partes.
- **Transferir el riesgo:** solo se puede transferir el riesgo porque no es posible realizar el tratamiento dado es del alcance de un tercero (pólizas de seguro, regionales, procesos).
- **Asumir o aceptar un 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 (memorando del dueño del riesgo) solamente para los riesgos que se encuentren en el nivel bajo.

Para la fase de tratamiento es necesario definir lo siguiente:

- Nombre de control.
- Responsable.
- Periodicidad
- Propósito.
- Tipo de control.
- Naturaleza del control.
- El control está documentado.
- Observaciones o desviaciones resultantes
- Evidencia de la ejecución del control.
- Riesgo emergente.
- Actividades.


Los estados de tratamiento se describen a continuación:

- **Atrasado:** cuando las actividades definidas no se están cumpliendo según las fechas establecidas.
- **Finalizado:** cuando el tratamiento ya se ejecutó.
- **En proceso:** cuando la ejecución de las actividades se encuentra acorde a las fechas establecidas

Mensualmente se realizará seguimiento y revisión al plan de tratamiento, recolección y verificación de evidencias de las actividades realizadas, teniendo en cuenta las fechas establecidas para su cumplimiento, así mismo se realizará el reporte del indicador según su periodicidad de medición

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



 BIENESTAR FAMILIAR	<b>PROCESO MEJORA E INNOVACION</b>	PL3.MI	31/01/2022
	<b>PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>	Versión 1	Página 9 de 12

### 3.6 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 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.

### 3.7 Oportunidad de Mejora

El Instituto Colombiano de Bienestar Familiar-ICBF no sólo deberá centrarse en los riesgos identificados, sino que este análisis o apreciación del riesgo debe ser la base para identificar oportunidades de mejora. Por lo anterior, la oportunidad deberá entenderse como la consecuencia positiva frente al resultado del tratamiento del Riesgo.

### 3.8 Materialización

En el caso de materializarse un riesgo, este debe ser reportado de acuerdo con el procedimiento de gestión de incidentes de seguridad de la información y en la matriz se deben identificar las actividades a seguir teniendo en cuenta los factores internos o externo que puede propiciar el riesgo. Asimismo, se deberá analizar el riesgo y validar en qué nivel queda posterior a la materialización, registrando los cambios respectivos en la matriz. 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 la matriz.

## 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:

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



**PROCESO  
MEJORA E INNOVACION**

PL3.MI

31/01/2022

**PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y  
PRIVACIDAD DE LA INFORMACIÓN**

Versión 1

Página 10 de  
12

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:

Tareas	Responsable de la Tarea	Entregable	Programación Tareas	
			Fecha inicio	Fecha final
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.	listado de asistencia o Listado de Asistencia de Microsoft Teams o Listados de asistencia por Microsoft Forms o Grabación de la sesión	31/01/2022	31/03/2022
Brindar orientación en la Identificación, Análisis y Evaluación 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  Matrices de Riesgos de los Procesos y Regionales	01/02/2022	31/03/2022

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



BIENESTAR FAMILIAR

**PROCESO  
MEJORA E INNOVACION**

PL3.MI

31/01/2022


**PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN**

Versión 1

Página 11 de 12

Tareas	Responsable de la Tarea	Entregable	Programación Tareas	
			Fecha inicio	Fecha final
Realizar la realimentación, revisión y verificación de los riesgos identificados con sus planes de tratamiento 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	01/03/2022	16/04/2022
Enviar las matrices de riesgos de las Regionales y SDG para Publicación en Intranet y Micrositio del Eje.	Profesional de la dirección de Información y Tecnología, encargado de la gestión de Riesgos de Seguridad de la Información.	Correo Electrónico	16/04/2022	20/04/2022
Realizar seguimiento a los riesgos identificados en la SDG y Regionales con sus planes de tratamiento	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	31/03/2022	20/12/2022
Realizar acompañamiento en la evaluación de riesgos residuales en la SDG y Regionales.	Gestor de riesgos SGSI, Profesional EPICO Referente SGSI - Ingeniero Regional	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	01/05/2021	20/12/2022
Actualizar la Guía Gestión de Riesgos Seguridad de la Información cuando sea necesario	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	01/07/2022	30/10/2022
Reportar el indicador de riesgos	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	01/04/2022	31/12/2022

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

 BIENESTAR FAMILIAR	<b>PROCESO MEJORA E INNOVACION</b>	PL3.MI	31/01/2022
	<b>PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>	Versión 1	Página 12 de 12

## 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 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	N/A	N/A

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