TABLA DE CONTENIDO

INTRODUCCIÓN

El plan de tratamiento de riesgos de Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación, se basa en una orientación estratégica que requiere el desarrollo de una cultura de carácter preventivo, de manera que, al comprender el concepto de riesgo, así como el contexto, se planean acciones que reduzcan la afectación a la entidad en caso de materialización, adicional se busca desarrollar estrategias para la identificación, análisis, tratamiento, evaluación y monitoreo de dichos riesgos con mayor objetividad, dando a conocer aquellas situaciones que pueden comprometer el cumplimiento de los objetivos trazados en favor de la niñez, adolescencia y las familias colombianas.

Lo anterior dando cumplimiento a la normativa establecida por el estado colombiano, CONPES 3854 de 2016, Modelo de Seguridad y Privacidad de MinTic y lo establecido en el decreto 1008 de 14 de junio 2018, adoptando las buenas prácticas y los lineamientos de los estándares ISO 27001:2013, ISO 31000:2018 y la guía para la administración del riesgo (DAFP).

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 de la Operación que el Instituto Colombiano de Bienestar Familiar ICBF pueda estar expuesto, y de esta manera alcanzar los objetivos, la misión y la visión institucional, protegiendo y preservando la integridad, confidencialidad, disponibilidad y autenticidad de la información.

1.1 OBJETIVOS ESPECIFICOS

- Cumplir con los requisitos legales y reglamentarios pertinentes a la legislación colombiana.

- Gestionar riesgos de Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación, de acuerdo con los contextos establecidos en la Entidad.

- Fortalecer y apropiar conocimiento referente a la gestión de riesgos Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación.

2. ALCANCE

Realizar una eficiente gestión de riesgos de Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación, que permita integrar en los procesos de la entidad, buenas prácticas que contribuyan a la toma de decisiones y prevenir incidentes que puedan afectar el logro de los objetivos. Junto con la guía de gestión de riesgos se dan los lineamientos para poder identificar, analizar, tratar, evaluar y monitorear los riesgos de seguridad y privacidad de la información en la Sede de la Dirección General y las 33 regionales del ICBF.

3. DESARROLLO

La gestión del riesgo no es una actividad independiente que se separa de las actividades y los procesos de la Entidad, la gestión del riesgo es parte de las responsabilidades de la alta dirección y una parte integral del nuevo modelo de operación por procesos, gestión de proyectos y gestión de cambios, incluyendo la planificación estratégica.

Para el desarrollo del plan de tratamiento de riesgos en el ICBF se debe poner en práctica lo definido en la guía de gestión, teniendo en cuenta los controles existentes los cuales deben ser revisados constantemente y la definición de nuevos controles a implementar (Anexos ISO 27001:2013). Por tal razón la entidad deberá diseñar y ejecutar estrategias para tratar los riesgos identificados de acuerdo con su criticidad (Niveles Altos, Moderados y Extremos) y opciones de tratamiento:

- Asumirlos o aceptarlos
- Reducirlos
- Evitarlos
- Compartirlos o transferirlos

Los riesgos con nivel de criticidad baja pueden ser asumidos o aceptados, aunque no se requiere hacer tratamiento, se deben identificar los controles existentes de tal manera que permitan ser evaluados y analizados ya que con base a los resultados se determinara si son adecuados o deberán modificarse.

Nota: se sugiere evaluar y cuantificar las posibles pérdidas que implicarían para la entidad la no adopción de medidas contra el riesgo.

Para la ejecución del plan de tratamiento de riesgos de Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación, se realizarán las actividades acordes a lo establecido y lo definido en el Plan de Implementación del SGSI.

3.1 RESPONSABILIDADES

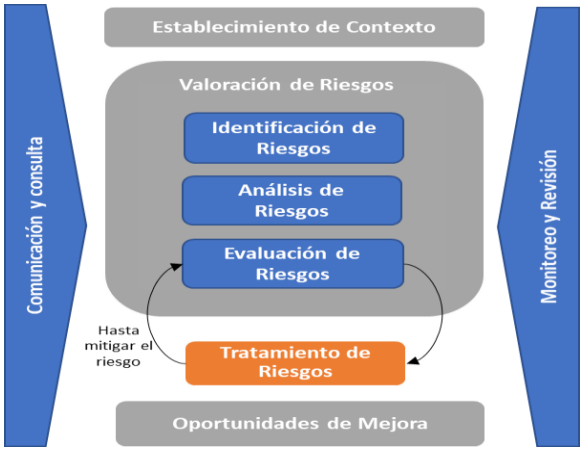
El ICBF deberá definir los roles y responsabilidades de todas las partes interesadas en lo concerniente a la gestión de riesgos, promoviendo el monitoreo y revisión a la gestión en sus etapas, con el propósito de asegurar el cumplimiento de los planes de tratamiento proyectados, ejecutando los controles 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.

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, de acuerdo con la identificación, análisis, valoración y tratamiento de estos de acuerdo con metodología establecida por la entidad descrita 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 de la Operación, como primera medida se establecen los siguientes roles:

- **Gestor de riesgos (SGSI):** Es el responsable de dirigir, coordinar y realizar seguimiento a la gestión en cada una de sus fases, en la Sede de la Dirección General, Regionales y Centros Zonales del ICBF.

- **Profesional EPICO:** Apoya la sostenibilidad y mejoramiento continuo del sistema integrado de gestión en la Sede de la Dirección General - Procesos.

- **Referente SIGE:** Apoya la sostenibilidad y mejoramiento continuo del sistema integrado de gestión en las regionales de acuerdo con el rol asignado.

- **Dueño del riesgo:** Es el responsable de contribuir con el seguimiento y control a la gestión de los riesgos identificados (aceptación de riesgos inherentes y residuales), además de la implementación de los controles definidos en la fase de tratamiento

3.3 Definición De Contexto

El Instituto cuenta con la Sede de la Dirección General, 33 regionales ubicadas en los 32 departamentos, 1 en el Distrito Capital de Bogotá y 213 Centros Zonales que hacen presencia en el ámbito municipal y local en todo el territorio nacional; llegando a más de 8 millones de colombianos con el servicio público de bienestar familiar, a través de sus programas y estrategias de atención.

3.4 Identificación y Análisis del Riesgo

Es necesario conocer los sucesos potenciales, estén o no bajo el control de la entidad que ponen en riesgo el logro de los objetivos establecidos para la institución, por lo que es preciso identificar las causas, la fuente y las consecuencias de su ocurrencia.

Para la identificación y descripción de los riesgos de Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la operación, se deben tener en cuenta los siguientes aspectos:

- Estar en términos cualitativos.
- Debe Incluir las causas y/o factores de riesgo y vulnerabilidades.

- Se debe determinar la afectación de alguno de los principios de la seguridad de la información.

  - Confidencialidad
  - Integridad
  - Disponibilidad
  - Seguridad y Privacidad
  - Continuidad de la Operación

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

- 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 la magnitud de los efectos que puede llegar a afectar los objetivos institucionales en caso que se materialice un riesgo.

3.5 Tratamiento

El propósito de esta etapa es la toma decisiones basadas en los resultados del análisis acerca de cuáles riesgos necesitan tratamiento y la prioridad para su manejo

De acuerdo con los resultados obtenidos en la fase de identificación, análisis y evaluación de riesgos, se definen los controles a implementar y sus características (Tipo, Naturaleza, Diseño, Ejecución y Efectividad), estableciendo una serie de actividades con el propósito de mitigar los riesgos identificados.

Los controles a implementar serán aquellos controles que el dueño de riesgo definirá para tratar los riesgos aceptados.

Para la fase de tratamiento es necesario definir lo siguiente:

- Actividades
- Fechas de ejecución (Inicio, terminación)
- Responsable
- Estado de tratamiento

Los estados de tratamiento se describen a continuación:

- **Atrasado:** cuando el tratamiento del riesgo no se está cumpliendo según las fechas establecidas.
- **Finalizado:** cuando el tratamiento ya se ejecutó.
- **En proceso:** cuando la ejecución del tratamiento 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, se debe relacionar las rutas que contienen dichas evidencias (Plan Operativo), sin embargo, se debe tener en cuenta reporte del indicador que se realizara cuatrimestralmente.

3.6 Evaluación

De acuerdo con el progreso obtenido y el seguimiento realizado en la fase de tratamiento de los riesgos, el gestor de riesgos en compañía del dueño del riesgo, calificaran los controles implementados teniendo en cuenta su diseño, ejecución y efectividad. Una vez determinada la calificación de los controles implementados, se procede a realizar la evaluación del nivel residual, para dicha evaluación nuevamente se determinará una Probabilidad X Impacto.

Nivel Inherente VS Nivel Residual.

- Si el resultado de la evaluación del nivel residual es Baja, se concluye que el riesgo fue mitigado y sus controles fueron adecuados.

- Si el resultado de la evaluación del nivel residual es moderado, alto o extremo, 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. Por lo anterior la oportunidad deberá entenderse como la consecuencia positiva frente al resultado del tratamiento del Riesgo.

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 de la Operación, 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 (Matriz de Riesgos SGSI)
Logísticos	Gestión de recursos para realizar socializaciones, transferencia de conocimientos y seguimiento a la gestión de riesgos.
Financieros	Recursos para la adquisición de conocimiento, recursos humanos, técnicos, y desarrollo de auditorías

5. TIEMPO DE EJECUCION

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:

N°	Actividades	N°	Tareas	Producto	Responsable de la tarea	Programación de Tareas	
						Fecha Inicio	Fecha Fin
1	Sensibilización	1	Socialización Guía y Herramienta - Gestión de Riesgos de Seguridad y privacidad de la Información, Seguridad Digital y Continuidad de la Operación	Actas de reunión, listados de asistencia - Video Conferencia Guía y herramienta de gestión	Gestor de Riesgos - equipo SGSI	15-ene-19	15-ene-19

2	Identificación de Riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y continuidad de la Operación	1	Identificación, Análisis y Evaluación de Riesgos - Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación SDG y regionales del ICBF	Matriz de riesgos, actas de reunión, correos electrónicos	Gestor de riesgos SGSI, Profesional EPICO Referente SGSI - Ingeniero Regional - Equipo SGSI	16-ene-19	28-ene-19
		2	Realimentación, revisión y verificación de los riesgos identificados (Ajustes)	Actas de reunión - Correos Electrónicos - Registro Bitácora Soporte a Regionales y Procesos, Video Conferencias	Gestor de riesgos SGSI, Profesional EPICO Referente SGSI - Ingeniero Regional - Equipo SGSI	28-ene-19	4-feb-19
3	Aceptación de Riesgos Identificados	1	Aceptación, aprobación Riesgos identificados y planes de tratamiento	Memorando Aceptación de riesgos Identificados - Matriz de riesgos, Plan de tratamiento	Líderes de Proceso / Director Regional	4-feb-19	8-feb-19
4	Publicación	1	Publicación Matriz de riesgos - Intranet y Micrositio del Eje	Matriz de riesgos publicada en la intranet de la regional	SMO	8-feb-19	13-feb-19
5	Seguimiento Fase de Tratamiento	1	Seguimiento Estado planes de tratamiento de riesgos identificados y verificación de evidencias	Actas de reunión, Memorandos, Correos electrónicos - evidencias del estado de tratamiento - Matriz de riesgos	Gestor de riesgos SGSI, Profesional EPICO Referente SGSI - Ingeniero Regional - Equipo SGSI	13-feb-19	31-dic-19
6	Evaluación de riesgos residuales	1	Evaluación de riesgos residuales	Actas de reunión, Correos electrónicos - Matriz de riesgos	Gestor de riesgos SGSI, Profesional EPICO Referente SGSI - Ingeniero Regional - Equipo SGSI	13-feb-19	31-dic-19
7	Mejoramiento	1	Identificación de oportunidades de mejora acorde a los resultados obtenidos durante la evaluación de riesgos residuales	Actas de reunión, Correos electrónicos - Matriz de riesgos	Gestor de riesgos SGSI, Profesional EPICO Referente SGSI - Ingeniero Regional - Equipo SGSI	13-feb-19	31-dic-19
		2	Actualización Guía Gestión de Riesgos Seguridad de la información, de acuerdo con los cambios solicitados.	Guía y Herramienta de Gestión de Riesgos	Gestor de Riesgos - equipo SGSI	14-may-18	24-jul-19

		3	Transición de riesgos identificados, conforme lo establecido en la nueva guía y herramienta Gestión de riesgos	Herramienta de Gestión - Matriz de riesgos actualizada - Actas de reunión	Gestor de riesgos SGSI, Profesional EPICO Referente SGSI - Ingeniero Regional - Equipo SGSI	15-ene-19	21-ene-19
8	Monitoreo y Revisión	1	Generación, presentación y reporte de indicadores de gestión SDG y Regionales del ICBF	Hoja de vida Indicador de eficacia gestión de riesgos SGSI	Gestor de riesgos SGSI, Profesional EPICO Referente SGSI - Ingeniero Regional - Equipo SGSI	La actividad se realizará cuatrimestralmente	

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 un indicador de gestión que está orientada principalmente en la medición de eficacia de los componentes de implementación y gestión definidos en el modelo de operación del marco de seguridad y privacidad de la información, indicador que se alimenta de indicadores internos en el marco de la implementación del Eje de Seguridad de la Información y que servirán como insumo para el componente de mejora continua permitiendo adoptar decisiones de mejora sobre el Eje de Seguridad de la información.

7.1 MEDICIÓN

La medición se realiza con un indicador de gestión que está orientada principalmente determinar el porcentaje de ejecución de actividades definidas en el tratamiento de riesgos de seguridad y privacidad de la información ubicados en zonas extremo, alto y moderado.

HOJA DE VIDA INDICADORES					
2019					
Fecha aprobación					
Fecha última modificación 2019-01-21					
Codigo Indicador:	**PA-142**				
Tipo Hoja:	**Porcentaje**				
Nombre:	Porcentaje de riesgos de seguridad de la información gestionados				
Objetivo:	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.				
INFORMACIÓN BASICA					
Linea Base:	0%	Meta Vigencia:	80%	Dato Nacional:	S
Periodicidad:	Cuatrimestral	Unidad de Medida:	Porcentaje	Dato Regional:	S
Tendencia:	Estatico	Ámbito de Medición:	Gestión	Dato Zonal:	
Dimensión de Medición:	Eficacia	Metas Sociales?:	N	Transversal?:	N
ALINEACIÓN GESTION INSTITUCIONAL					
Objetivo Institucional:	Asegurar una gestión institucional, orientada a resultados a nivel nacional y regional, apoyada en el uso de las tecnologías de la información				
Perspectiva Mapa Estratégico:	Pp.Gestionar el conocimiento institucional, con sistemas de información integrados y seguros				
Código del Proceso:	PT3	Nombre del Proceso	Gestión de la tecnología e información		
Objetivo SIGE:	SIGE10	Nombre SIGE	Gestionar el conocimiento institucional, con sistemas de información confiables, integrados y disponibles.		
ALINEACIÓN ESTRATEGIA					
Plan de Acción					
Código Dimensión:	D3		Nombre Dimensión:	GESTIÓN CON VALORES PARA EL RESULTADO	
Código Política:	D3P7		Nombre Política:	GOBIERNO DIGITAL: TIC para la gestión y Seguridad de la información	
Plan Institucional y/o Estratégico:	Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Informacion				
Proyecto de Inversion:	C-4199-1500-7				
Plan Indicativo:	S		Meta Cuatrienio:	NA	
Meta Plan de Acción:	80%				
METODOLOGIA DE MEDICIÓN					
Cálculo del Numerador:	Número de actividades ejecutadas a la fecha de corte		Fuente del Numerador:	Matriz de riesgos Sede de la Dirección General y Regional	
Cálculo del Denominador :	Número de actividades programadas a la fecha de corte		Fuente del Denominador:	Matriz de riesgos Sede de la Dirección General y Regional	
Descripción de la Meta:	Alcanzar el 80% de la gestión de riesgos de seguridad de la información.		Fuente de la Meta:	Acta de definición metas	
ASPECTOS TECNICOS					

Definición de Términos:	AMENAZA: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. ANÁLISIS DEL RIESGO: Proceso para comprender la naturaleza del riesgo. CONTROL: Medida que modifica el riesgo. DUEÑO DEL RIESGO: Persona o entidad con la responsabilidad de rendir cuentas y la autoridad para gestionar un riesgo. IMPACTO: Magnitud del daño, efectos al generarse si se materializa el riesgo. NIVEL DE RIESGO: Magnitud de un riesgo o de una combinación de riesgos, expresada en términos de la combinación de las consecuencias y su probabilidad. PROBABILIDAD: Análisis cualitativo que permite determinar la ocurrencia. RIESGO: Efecto de la incertidumbre sobre los objetivos. RIESGO INHERENTE: Es propio del proceso o la actividad RIESGO RESIDUAL: Riesgo remanente después del tratamiento del riesgo. Para mayor detalle consultar la Guía de Gestión de Riesgos y Peligros G3.MI.
Aplicó Vigencia Anterior?:	S
Codigo Vigencia Anterior:	A11-PT3-04
Nombre Vigencia Anterior:	Porcentaje de eficacia del SGSI
Area Responsable:	Dirección de Información y Tecnología
Mecanismo de Control:	1. Se definió la Dirección de Información y Tecnología como única fuente que genera y suministra los datos del indicador. 2. Dentro de la Dirección de Información y Tecnología se realiza una verificación adicional. 3. Las inquietudes que surjan entorno al indicador deben ser escaladas a la Dirección de Información, quienes serán los únicos autorizados para verificar y responder.

RANGOS VALORACIÓN									
Mes de Inicio:	Abril				Dato con Rezago? :				
Mes	Critico		En riesgo		Adecuado		Optimo		
Mes	Min	Max	Min	Max	Min	Max	Min	Max	
Abril	%	%	%	%	%	%	%	%	
Agosto	%	%	%	%	%	%	%	%	
Diciembre	%	%	%	%	%	%	%	%	
Observaciones									

8. DOCUMENTOS DE REFERENCIA:

- G3.MI Guía de Gestión de Riesgos y Peligros

9. CONTROL DE CAMBIOS

Fecha	Versión	Descripción del Cambio
24/10/2018	PL1.MI Versión 1	Elaboración del documento.
	PL1.MI Versión 2	Se realizan ajustes al contenido de los siguientes numerales: INTRODUCCIÓN 1.OBJETIVO GENERAL 1.1 OBJETIVOS ESPECIFICOS 2. ALCANCE 3. DESARROLLO 3.1 RESPONSABILIDADES 3.2 METODOLOGÍA 3.3 Definición De Contexto 3.4 Identificación y Análisis Del Riesgo 3.5 Tratamiento 3.6 Evaluación 3.7 Oportunidad de Mejora 4. RECURSOS 5. TIEMPO DE EJECUCION 6. PRESUPUESTO 7. MEDICIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Elaboró	*Revisó*	*Aprobó*
Profesionales contratistas Eje de Seguridad de la Información Dayana Carbonó Carbonó Teresa Quilindo Sarasti John J. Enciso Alarcon Juan N. Ayala Rodriguez Hernan D. Fagua Yanquen Jose G. Rodriguez Duarte	**Andrés Díaz Molina** Contratista Líder de implementación Eje de Seguridad de la Información	**Piedad Cecilia Montero Villegas** Directora de Información y Tecnología Líder del Eje de Seguridad de la Información **Comité Institucional de Gestión y Desempeño** Competencia por Resolución 6970 de 2018 Sesión ordinaria #001 del 24 de enero de 2019