

 BIENESTAR FAMILIAR	PROCESO MEJORA E INNOVACIÓN	PL2.MI	30/01/2021
	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Versión 1	Página 1 de 12

TABLA DE CONTENIDO

INTRODUCCIÓN	2
1. OBJETIVO GENERAL	2
1.1 Objetivos Específicos.....	2
2. ALCANCE	3
3. DESARROLLO	3
3.1 Responsabilidades	4
3.2 Metodología.....	4
3.3 Definición de Contexto.....	5
3.4 Identificación, Análisis y Valoración del Riesgo	5
3.5 Tratamiento.....	6
3.6 Evaluación	7
3.7 Oportunidad de Mejora.....	8
3.8 Materialización	8
4. RECURSOS	8
5. TIEMPO DE EJECUCIÓN	9
6. PRESUPUESTO	10
7. MEDICIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	10
7.1 Medición.....	11
8. DOCUMENTOS DE REFERENCIA:	12
9. CONTROL DE CAMBIOS	12

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

 BIENESTAR FAMILIAR	PROCESO MEJORA E INNOVACIÓN	PL2.MI	30/01/2021
	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Versión 1	Página 2 de 12

INTRODUCCIÓN

La gestión de riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación Tecnológica, 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 de MinTic 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 de la Operación Tecnológica que el Instituto Colombiano de Bienestar Familiar 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 Específicos

- 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 Tecnológica, de acuerdo con el contexto en la Entidad
- Fortalecer y apropiar el conocimiento referente a la gestión de riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación Tecnológica.

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

 BIENESTAR FAMILIAR	PROCESO MEJORA E INNOVACIÓN	PL2.MI	30/01/2021
	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Versión 1	Página 3 de 12

2. ALCANCE

La gestión de riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación Tecnológica aplica en 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, así mismo, hacen parte de las responsabilidades de la alta dirección.

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, tratar, valorar, evaluar y monitorear los riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación Tecnológica 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

- **Asumirlos o Aceptarlos:** Decisión de aceptar las consecuencias y probabilidad de un riesgo en particular, retener el riesgo mediante una decisión informada, solamente para los riesgos que se encuentren en el nivel bajo (memorando del dueño del riesgo)
- **Reducirlos:** Tomar medidas encaminadas a disminuir tanto la probabilidad (medidas de prevención), como el impacto (medidas de protección).
- **Evitarlos:** Tomar las medidas encaminadas a prevenir su materialización, decidir no iniciar o continuar la actividad que lo originó
- **Compartirlos o Transferirlos:** Reduce su efecto compartiéndolo con una o varios de los procesos o partes, (incluyendo los contratos y la financiación del riesgo).

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.

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

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

 BIENESTAR FAMILIAR	PROCESO MEJORA E INNOVACIÓN	PL2.MI	30/01/2021
	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Versión 1	Página 4 de 12

Para la ejecución del plan de tratamiento de riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación Tecnológica, se realizarán las actividades acordes a lo establecido en el Plan de Sostenibilidad del Modelo 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 asegurar el cumplimiento de los planes de tratamiento proyectados, ejecutando los controles y acciones definidos, desarrollando e implementando procesos de control y gestión con el propósito de asegurar la efectividad y el cumplimiento de los objetivos institucionales.

Dichas responsabilidades son acordes a la 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 y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación Tecnológica, de acuerdo con la identificación, análisis, valoración y tratamiento de estos de acuerdo con la metodología establecida por la entidad, descrita a continuación:

Figura 1: Metodología de Gestión de Riesgos



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

 BIENESTAR FAMILIAR	PROCESO MEJORA E INNOVACIÓN	PL2.MI	30/01/2021
	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Versión 1	Página 5 de 12

Para la gestión de riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación Tecnológica, 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 sus fases de identificación, tratamiento, evaluación y oportunidades de mejora para las diferentes sedes 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 aprobación de los controles definidos en la fase de tratamiento. Para el ICBF, el dueño del riesgo es el líder del proceso y en el Formato Matriz de Riesgos SGSI, este se identifica en la casilla PROCESO, teniendo en cuenta sus objetivos y contextos.

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 215 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, Análisis y Valoración 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, así mismo es importante identificar los cambios que se presenten en el contexto externo e interno de la entidad.

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

- Estar en términos cualitativos.

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

 BIENESTAR FAMILIAR	PROCESO MEJORA E INNOVACIÓN	PL2.MI	30/01/2021
	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Versión 1	Página 6 de 12

- 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 de que se materialice un riesgo.

Para la Valoración del Riesgo de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación Tecnológica, se debe tener en cuenta el tabulador resultado del consolidado de los riesgos de la vigencia.

3.5 Tratamiento

El propósito de esta etapa es la toma de 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 para 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

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

	PROCESO MEJORA E INNOVACIÓN PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	PL2.MI	30/01/2021
		Versión 1	Página 7 de 12

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

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 cada cuatro meses se realiza el reporte del indicador.

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, calificarán 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 por Impacto.

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.

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

 BIENESTAR FAMILIAR	PROCESO MEJORA E INNOVACIÓN	PL2.MI	30/01/2021
	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Versión 1	Página 8 de 12

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, éste 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. Así mismo, 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 referente SGSI 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 de la Operación Tecnológica, 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

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

 BIENESTAR FAMILIAR	PROCESO MEJORA E INNOVACIÓN	PL2.MI	30/01/2021
	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Versión 1	Página 9 de 12

5. TIEMPO DE EJECUCIÓN

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:

Actividades	Tareas	Responsable de la tarea	Programación de Tareas	
			Fecha Inicio	Fecha Fin
Sensibilización	Socializar la Guía y Herramienta - Gestión de Riesgos de Seguridad y privacidad de la Información, Seguridad Digital y Continuidad de la Operación Tecnológica en la SDG y Regionales	Gestor de Riesgos - equipo SGSI	18-ene-21	31-mar-21
Identificación, Análisis y Valoración del Riesgo	Brindar apoyo en la Identificación, Análisis, Valoración y Evaluación de los Riesgos - Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación tecnológica en la SDG y Regionales	Gestor de riesgos SGSI, Gestor de continuidad, Equipo SGS	1-feb-21	31-mar-21
	Realizar la realimentación, revisión y verificación de los riesgos identificados con sus planes de tratamiento en la SDG y Regionales	Gestor de riesgos SGSI, Equipo SGSI	1-mar-21	31-mar-21
Aceptación de Riesgos Identificados	Proyectar y enviar documento base de aceptación de los riesgos y verificar la aprobación de los riesgos identificados en la SDG y Regionales	Gestor de riesgos SGSI, Equipo SGSI	31-mar-20	9-abr-21
Publicación	Enviar las matrices de riesgos de las Regionales y SDG para Publicación en Intranet y Micrositio del Eje	Gestor de riesgos SGS	12-abr-21	16-abr-21

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

 BIENESTAR FAMILIAR	PROCESO MEJORA E INNOVACIÓN	PL2.MI	30/01/2021
	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Versión 1	Página 10 de 12

Seguimiento Fase de Tratamiento	Realizar seguimiento a los riesgos identificados en la SDG y Regionales con sus planes de tratamiento	Gestor de riesgos SGSI, Equipo SGSI	8-mar-21	20-dic-21
Evaluación de riesgos residuales	Realizar acompañamiento en la evaluación de riesgos residuales en la SDG y Regionales	Gestor de riesgos SGSI, Equipo SGSI	17-abr-21	20-dic-21
Mejoramiento	Realizar acompañamiento en la evaluación de riesgos residuales	Gestor de riesgos SGSI, Profesional EPICO Referente SGSI - Ingeniero Regional - Equipo SGSI	1-jul-21	20-dic-21
	Revisar la Guía Gestión de Riesgos Seguridad de la información y realizar la actualización en caso de que se requiera.	Gestor de Riesgos SGSI, Equipo SGSI	01-jul-21	30-sep-21
Monitoreo y Revisión	Reportar el indicador de riesgos	Gestor de Riesgos SGSI, 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 a través de un indicador de gestión que está orientado principalmente en la medición de la 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.

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

 BIENESTAR FAMILIAR	PROCESO MEJORA E INNOVACIÓN	PL2.MI	30/01/2021
	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Versión 1	Página 11 de 12

7.1 Medición

La medición se realiza con un indicador de gestión que está orientado principalmente a 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					
Código 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 BÁSICA					
Línea Base:	0%	Meta Vigencia:	80%	Dato Nacional:	S
Periodicidad:	Cuatrimstral	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 GESTIÓN 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 Información				
Proyecto de Inversión:	C-4199-1500-7				
Plan Indicativo:	S	Meta Cuatrienio:	NA		
Meta Plan de Acción:	80%				
METODOLOGÍA 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 TÉCNICOS					

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



**PROCESO
MEJORA E INNOVACIÓN**

PL2.MI

30/01/2021

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

Versión 1

Página 12 de
12

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								
Código 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	Crítico		En riesgo		Adecuado		Óptimo		
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
N/A	N/A	N/A

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