INSTITUTO COLOMBIANO DE BIENESTAR FAMILIAR - ICBF

GUÍA GESTIÓN DE RIESGOS Y PELIGROS

PÚBLICA

TABLA DE CONTENIDO

INTRODUCCIÓN 5
1. GENERALIDADES 6
2. GESTIÓN DE RIESGOS – CALIDAD, FISCAL Y CORRUPCIÓN 8
2.1 Gestión de Riesgos de Procesos (Calidad, Fiscal y Corrupción) 9
2.1.1. Establecer el Contexto 10
2.1.2 Metodología para la identificación del contexto 11
2.1.3. Identificación del Riesgo 11
2.1.4. Análisis de Insumos 12
2.1.5. Identificación de Áreas de Impacto 12
2.1.6. Identificación Puntos de Riesgos de Calidad y Fiscales 13
2.1.7. Identificación Factores de Riesgos 15
2.1.8. Descripción de Riesgo de Calidad y Fiscales 15
2.1.9. Descripción de Riesgo de Corrupción 17
2.1.10. Clasificación de Riesgos 18
2.1.11. Determina el nivel de aplicabilidad del riesgo 18
2.1.12. Valoración de Riesgos de Calidad 18
2.1.13. Análisis de Riesgo 19
2.1.14. Evaluación de Riesgos de Calidad 22
2.1.15 Valoración Riesgos de Corrupción 27
2.1.16. Monitoreo y Revisión 36
2.1.17. Monitoreo y Seguimiento Riesgos de Corrupción 38
2.1.18. Comunicación y Consulta 38
3. GESTIÓN DE PELIGROS DE SEGURIDAD Y SALUD EN EL TRABAJO 39
3.1. Objetivos Específicos 39
3.2. Políticas operacionales para la identificación de peligros, valoración de riesgos y determinación de los controles de Seguridad y Salud en el Trabajo y Plan Estratégico de Seguridad Vial 40
3.3. Responsabilidad y Autoridad 41
3.4. Metodología 41
4. GESTIÓN DE RIESGOS Y OPORTUNIDADES SISTEMA DE GESTIÓN DE SEGURIDAD Y SALUD EN EL TRABAJO – SGSST 54

PÚBLICA

4.1. Políticas Operativas para la Gestión de Riesgos y Oportunidades para el Sistema de Gestión de la Seguridad y Salud en el Trabajo: 54
4.2. Seguimiento y reporte 56
5. GESTIÓN DE RIESGOS DE EMERGENCIA 56
5.1. Objetivo General 56
5.2. Condiciones Generales 57
5.3. Identificación de Amenazas 57
5.4. Metodología de Análisis Preliminar de Riesgos 58
5.5. Factores que Afectan la Amenaza y el Riesgo 59
5.6. Valorización de las Consecuencias 59
5.7. Elementos de Gestión en Seguridad y Salud 60
5.8. Aspectos Ambientales 62
5.9. Otros Aspectos 62
5.10. Matriz de Riesgos 63
5.11. Formato de Evaluación 64
5.12. Otras Metodologías 65
6. GESTION DE RIESGOS AMBIENTALES 65
6.1. Objetivos 66
6.2. Políticas Operativas para la Gestión de Riesgos del Eje Ambiental 66
6.3. Identificación del Riesgo 68
6.3.1 Análisis de Insumos 69
6.3.2 Identificación de Áreas de Impacto 69
6.3.3 Identificación de puntos de riesgos 69
6.3.4 Identificación de puntos de riesgos 70
7. GESTION DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION, CIBERSEGURIDAD, Y CONTINUIDAD DE LA OPERACIÓN. 79
7.1. Objetivos 79
7.2. Condiciones Generales 80
7.3. Identificación de riesgos de activos de información priorizados 83
7.3.1. Establecimiento del alcance, contexto y criterios 83
7.3.2. Codificación y Redacción de riesgos de Seguridad y Privacidad de la información, ciberseguridad y Continuidad de la Operación 84
7.3.3. Identificación de Activos de Información Priorizado 86

PÚBLICA

7.3.4. Identificación de consecuencias positivas y negativas. 87
7.3.5. Clasificación riesgos 87
7.4. Análisis del Riesgo 88
7.5. Valoración del riesgo 90
7.6. Manejo del riesgo 92
7.7. Monitoreo 94
7.8. Evaluación del riesgo residual: 94
7.9. Oportunidad de Mejora 95
7.10. Materialización 95
8. ANEXOS 95
9. FORMATOS 95
10. CONTROL DE CAMBIOS 96

PÚBLICA

INTRODUCCIÓN

La planeación con un enfoque basado en riesgos 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 de contexto, se pueda influir en el logro de los objetivos institucionales y planear acciones que reduzcan la probabilidad de ocurrencia de estos.

La adopción y aplicación de una serie de principios frente a riesgos, así como la definición de un marco de referencia y el desarrollo de un proceso consistente y sistemático, permite que la gestión del riesgo sea un ejercicio que establezca una base confiable para la toma de decisiones, que aumente la probabilidad de alcanzar los objetivos planificados, prevengan actos de corrupción, mejore la eficacia y la eficiencia operativa de los procesos a través de la minimización o prevención de pérdidas y gestión de incidentes, entre otros aspectos.

Esta guía describe la metodología establecida por el Instituto Colombiano de Bienestar Familiar para la gestión del riesgo en los cuatro ejes del Sistema Integrado de Gestión (Calidad, Ambiental, Seguridad y Salud en el Trabajo y Seguridad de la Información), de tal forma que los colaboradores cuenten con los elementos que orientan el entendimiento de la gestión del riesgo en la entidad.

Mediante la aplicación de esta guía la entidad busca realizar de manera objetiva y precisa la identificación, valoración, tratamiento y monitoreo de los riesgos para el cumplimiento de los objetivos trazados en favor de los niños, niñas, adolescentes, así como el fortalecimiento de las capacidades de los jóvenes y las familias que se encuentran en el territorio colombiano.

PÚBLICA

1. GENERALIDADES

OBJETIVO

Establecer directrices metodológicas para gestionar de forma integral los riesgos significativos y peligros a los que se encuentra expuesto el Instituto Colombiano de Bienestar Familiar, mitigando la probabilidad de materialización de estos y afectación de los objetivos institucionales.

ALCANCE

La presente guía aplica a la gestión de los riesgos significativos y peligros de los procesos de la Entidad, a los que podría estar expuesto el ICBF en la Sede de la Dirección **General**, las Direcciones Regionales y los Centros Zonales.

MARCO DE REFERENCIA

El instituto cuenta con una política de riesgos que promueve la gestión integral del riesgo, propiciando espacios permanentes de comunicación, revisión, seguimiento y control a los planes de tratamiento para perseverar en el desarrollo y protección integral de los niños, niñas, adolescentes, así como el fortalecimiento de las capacidades de los jóvenes y las familias como entornos protectores y principales agentes de transformación social.

Con la gestión del riesgo se busca fortalecer las medidas de prevención y control de las actividades desarrolladas en el ICBF, de acuerdo con la identificación, análisis, valoración y tratamiento de estos.

La Dirección de Planeación y Control de Gestión a través de la Subdirección de Mejoramiento Organizacional brinda a los líderes y responsables de los procesos las orientaciones para la aplicación de la metodología de gestión del riesgo en particular lo relacionado con calidad y corrupción, igualmente, la Dirección de Gestión Humana, la Dirección de Información y Tecnología y la Dirección Administrativa brindan orientaciones para la identificación de riesgos y peligros correspondientes a los ejes de Seguridad y Salud en el Trabajo, Seguridad de la Información y Ambiental; además de facilitar el seguimiento y actualización de los riesgos, en la medida que cambien los contextos: interno, externo y de proceso.

Para la gestión de los riesgos y peligros en el ICBF se toman en cuenta principalmente los siguientes documentos:

- ✓ Ley 1474 de 2011 articulo 73 Plan Anticorrupción y de Atención al Ciudadano
- ✓ Ley 1581 de 2012. “Por la cual se dictan disposiciones generales para la protección de datos personales”
- ✓ Ley 1523 de 2012. “Por la cual se adopta la política nacional de gestión del riesgo de desastres y se establece el Sistema Nacional de Gestión del Riesgo de Desastres y se dictan otras disposiciones”
- ✓ Ley 1712 de 2014. “Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones”
- ✓ Decreto 1072 de 2015. “Por medio del cual se expide el Decreto Único Reglamentario del Sector Trabajo”

PÚBLICA

- ✓ Resolución 312 de 2019 “Por la cual se definen los Estándares Mínimos del Sistema de Gestión de la Seguridad y Salud en el Trabajo SG-SST”
- ✓ Norma NTC ISO 22301: 2012 Sistema de Gestión de Continuidad de Negocio
- ✓ Norma NTC ISO 27001:2022 Sistema de Gestión de Seguridad de la Información, Ciberseguridad y Protección de la Privacidad
- ✓ Norma NTC ISO 14001:2015 Sistema de Gestión Ambiental
- ✓ Norma NTC ISO 9001: 2015 Sistema de Gestión de la Calidad
- ✓ Norma NTC ISO 45001:2018 Sistemas de Gestión de la Seguridad y Salud en el Trabajo.
- ✓ Norma Técnica Colombiana NTC ISO 31000:2018. Gestión del Riesgo
- ✓ GTC 45 Guía Técnica Colombiana para la Identificación de los Peligros y la Valoración de los Riesgos en Seguridad y Salud Ocupacional - 2015
- ✓ CONPES 3854 de 2016 – Política Nacional de Seguridad Digital
- ✓ Decreto 124 del 26 de enero de 2016. - Por el cual se sustituye el Titulo 4 de la Parte 1 del Libro 2 del Decreto 1081 de 2015, Relativo al "Plan Anticorrupción y de Atención al Ciudadano".
- ✓ Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas Riesgos de Gestión, Corrupción y seguridad Digital – Departamento Administrativo de la Función Pública – DAFP - octubre 2018.
- ✓ Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas – Departamento Administrativo de la Función Pública – DAFP - noviembre 2022.
- ✓ Ley 2195 de 2022 del 18 de enero. “Por medio de la cual se adoptan medidas en materia de transparencia, prevención y lucha contra la corrupción y se dictan otras disposiciones”.
- ✓ Decreto 1499 de 2017 del 11 de septiembre “Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015”
- ✓ Modelo de Seguridad y Privacidad de la Información de MinTic – 2016.
- ✓ Resolución 40595 del 2022 “Por la cual se adopta la metodología para el diseño, implementación y verificación de los Planes Estratégicos de Seguridad Vial y se dictan otras disposiciones”.

BENEFICIOS[1]

- ✓ Aumentar la probabilidad de alcanzar los objetivos
- ✓ Fomentar la gestión proactiva
- ✓ Mejorar el gobierno
- ✓ Mejorar la confianza de las partes interesadas
- ✓ Establecer una base confiable para la toma de decisiones y la planificación
- ✓ Mejorar los controles
- ✓ Mejorar la eficacia y la eficiencia operativa
- ✓ Minimizar las pérdidas
- ✓ Mejorar el aprendizaje organizacional

1 Tomado de NTC ISO 31000:2018

PUBLICA

PRINCIPIOS[2]

a) Integrada: La gestión del riesgo es parte integral de todas las actividades de la entidad.

b) Estructurada y exhaustiva: Un enfoque estructurado y exhaustivo hacia la gestión del riesgo contribuye a resultados coherentes y comparables.

c) Adaptada: El marco de referencia y la gestión del riesgo se adapta y es proporcional a los contextos externo e interno del Instituto y se relaciona con sus objetivos.

d) Inclusiva: La participación apropiada y oportuna de las partes interesadas pertinentes permite que se consideren su conocimiento, puntos de vista y percepciones. Esto resulta en una mayor toma de conciencia y una gestión del riesgo informada, en especial en relación con riesgos de corrupción.

e) Dinámica: Los riesgos pueden aparecer, cambiar o desaparecer con los cambios de los contextos externo e interno de la organización. La gestión del riesgo anticipa, detecta, reconoce y responde a esos cambios y eventos de una manera apropiada y oportuna.

f) Mejor información disponible: Las entradas a la gestión del riesgo se basan en información histórica y actualizada, así como en expectativas.

g) Mejora continua: La gestión del riesgo mejora continuamente mediante el aprendizaje y experiencia de los colaboradores del ICBF.

2. GESTIÓN DE RIESGOS – CALIDAD, FISCAL Y CORRUPCIÓN

La gestión del riesgo para el Instituto Colombiano de Bienestar Familiar en todos procesos y niveles (Sede la Dirección General, Regional y Zonal) es un elemento de la planeación estratégica, así como de la gestión cotidiana, dado el contexto externo e interno en el que se desenvuelve y la particularidad del servicio que presta a las niñas, niños, adolescentes, jóvenes y familias que se encuentren en el territorio colombiano.

Convencidos de que la adecuada gestión del riesgo en los procesos permite aumentar la probabilidad de alcanzar los objetivos institucionales, la entidad revisa y mejora de manera periódica su metodología y herramienta, aumentando el nivel de objetividad para el análisis de elementos tales como la probabilidad y el impacto de los riesgos, así como para la evaluación de los controles existentes que ayudan mitigar los riesgos identificados.

La metodología para la gestión de riesgos por procesos de calidad y corrupción se basa en la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas versión 6 de 2022 y versión 4 de 2018 del Departamento Administrativo de la Función Pública, así como la Norma Técnica ISO 31000 versión 2018.

2 Tomado de NTC ISO 31000:2018

PÚBLICA

Adicional a lo anterior también es pertinente mencionar y definir el Control Fiscal Interno el cual es el primer nivel para la vigilancia fiscal de los recursos públicos y para la prevención de riesgos fiscales y defensa del patrimonio público. El Control Fiscal Interno, hace parte del Sistema de Control Interno y es responsabilidad de todos los servidores públicos y de los particulares que administran recursos, bienes, e intereses patrimoniales de naturaleza pública y de las líneas de defensa, en lo que corresponde a cada una de ellas. El Control Fiscal Interno es evaluado por la Contraloría, siendo dicha evaluación determinante para el fenecimiento de la cuenta.

OBJETIVO

Establecer la metodología para gestionar los riesgos de calidad, fiscales y corrupción identificados en el marco de los procesos de la entidad en todos sus niveles.

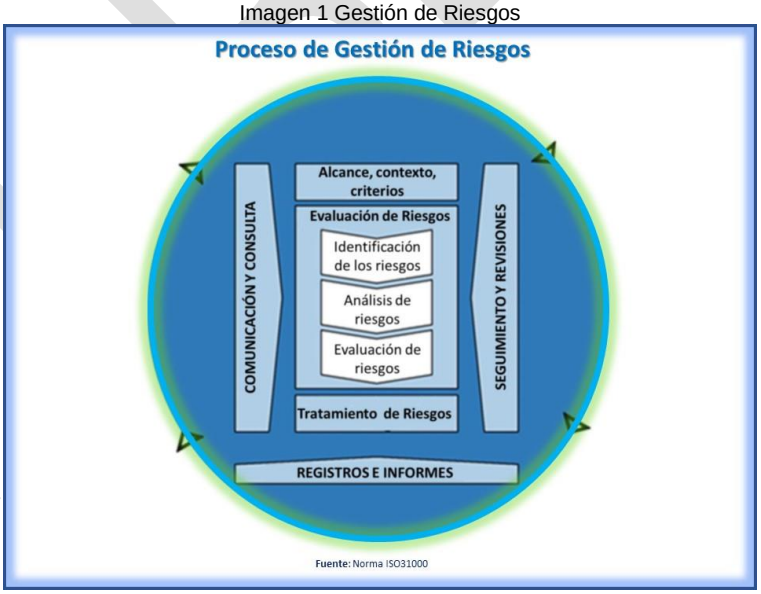
2.1 Gestión de Riesgos de Procesos (Calidad, Fiscal y Corrupción)

La gestión de riesgos del ICBF se realiza con base en lo establecido en los siguientes documentos de referencia:

- Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas. Departamento Administrativo de la Función Pública.
- Norma Técnica Colombiana NTC ISO 31000:2018

La gestión de riesgos por procesos de calidad y corrupción comprende las fases descritas en la siguiente imagen:

Imagen 1 Gestión de Riesgos



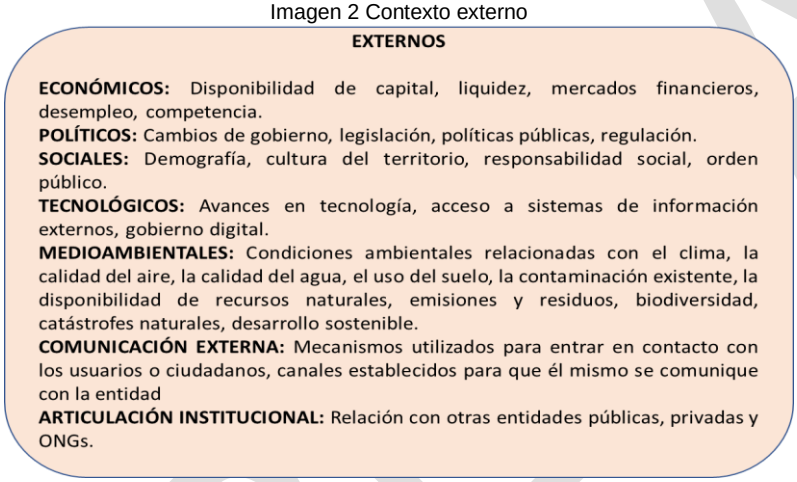
PÚBLICA

2.1.1. Establecer el Contexto

El contexto en términos generales relaciona los aspectos externos, internos y del proceso que se deben tener en cuenta para gestionar los riesgos de la entidad. A partir del contexto es posible establecer las causas de los riesgos a identificar.

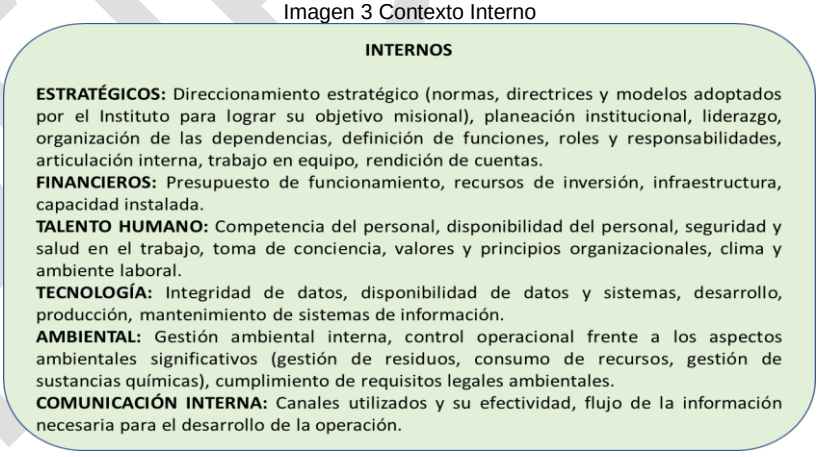
Contexto Externo: Se determinan las características o aspectos esenciales del entorno en el cual opera la entidad. Se pueden considerar factores como:

Imagen 2 Contexto externo



Contexto Interno: Se determinan las características o aspectos esenciales del entorno en el cual la organización busca alcanzar sus objetivos. Se pueden considerar factores como:

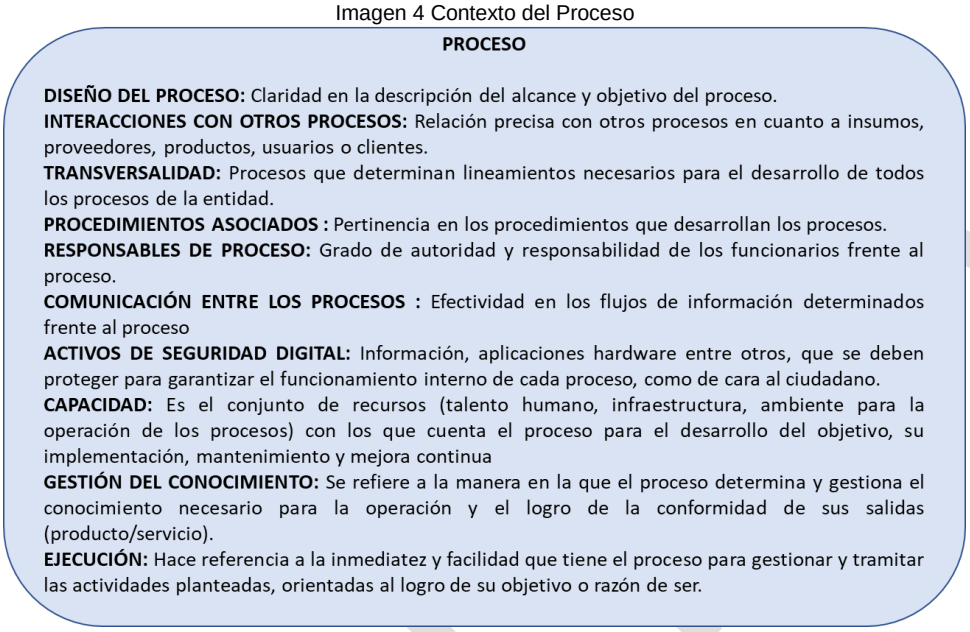
Imagen 3 Contexto Interno



PRUEBA

Contexto del Proceso: Se determinan las características o aspectos esenciales del proceso y sus interrelaciones. Se pueden considerar factores como:

Imagen 4 Contexto del Proceso



2.1.2 Metodología para la identificación del contexto

El ICBF apropió para el análisis de su contexto la metodología DOFA (Debilidades – Oportunidades – Fortalezas – Amenazas), la cual consiste en identificar aquellas cuestiones del entorno (contexto externo): amenazas (riesgo negativo) y oportunidades (riesgo positivo) y al interior de la entidad en los tres niveles (contexto interno): debilidades (riesgo negativo) y fortalezas (riesgo positivo) que pueden, bien sea fortalecer y/o mejorar la gestión institucional o afectar el cumplimiento de los objetivos de la entidad.

Esta metodología se implementa anualmente en los tres niveles de la entidad (Nacional, Regional y Zonal) de acuerdo con lo establecido en el P22.DE Procedimiento Identificación y Actualización del Contexto Interno y Externo ICBF.

2.1.3. Identificación del Riesgo

Es la etapa inicial de la gestión de riesgos de la entidad y tiene como objetivo identificar los riesgos significativos que deben ser gestionados teniendo en cuenta su impacto negativo en la consecución de los objetivos estratégicos y de procesos, para ello se deben considerar el contexto estratégico tanto interno como externo, así como las caracterizaciones de los procesos definidos por la entidad.

Para el desarrollo de esta etapa se deben tener en cuenta lo siguiente:

- Análisis de Insumos
- Identificación de Áreas de Impacto
- Identificación de Puntos de Riesgo
- Identificación de Factores de Riesgo

- Descripción del Riesgo
- Definición Riesgos de Corrupción
- Clasificación de Riesgos
- Determinar el Nivel de Aplicabilidad del riesgo

2.1.4. Análisis de Insumos

Para iniciar con la identificación de riesgos es necesario analizar los siguientes insumos:

- Misión de la entidad.
- Objetivos estratégicos.
- Objetivos de los procesos.
- Plan Indicativo Institucional.
- Plan de Acción Institucional.
- Análisis de contexto interno y externo.
- Necesidades y expectativas de las partes interesadas.
- Resultados de la gestión de riesgos de la vigencia anterior.
- Informes entes de control.
- Informe denuncias presuntos actos de corrupción.
- Resultados validación de riesgos con regionales y centros zonales.
- Recomendaciones informes Oficina de Control Interno

2.1.5. Identificación de Áreas de Impacto

Son aquellas consecuencias a las cuales se ve expuesta la entidad cuando se produce la materialización de un riesgo, estas áreas de impacto pueden ser:

- **Afectación Económica:** pérdida de recursos económicos.
- **Reputacional:** afectación de la imagen y/o credibilidad Institucional.
- **Cumplimiento Objetivos del Proceso:** afectación en el cumplimiento o consecución del objetivo del proceso.

Dentro del contexto de riesgo fiscal, el área de impacto **siempre corresponderá a una consecuencia económica sobre el patrimonio público**, a la cual se vería expuesta la entidad en caso de materializarse el riesgo. Es importante, tener en cuenta que no todos los efectos económicos corresponden a riesgos fiscales, **pero todos los riesgos fiscales representan un efecto económico**.

Son ejemplo de efectos económicos que no son riesgos fiscales, los siguientes:

- Los riesgos de daño antijurídico -riesgo de pago de condenas y conciliaciones.

- Los efectos económicos generados por causas exógenas, es decir, no relacionadas con acción u omisión de los gestores públicos, como son hechos de fuerza mayor, caso fortuito o hecho de un tercero (es decir, de alguien que no tenga la calidad de gestor público (ver definición de gestor público en el capítulo uno de conceptos básicos).

PÚBLICA

2.1.6. Identificación Puntos de Riesgos de Calidad y Fiscales

En el marco del flujo de los procesos se deben identificar aquellas actividades críticas que pueden provocar la materialización de un riesgo y deben ser controladas. A partir de los puntos de riesgo se realizará en la etapa de valoración la determinación de la probabilidad de ocurrencia. La identificación de puntos de riesgo solo aplica a riesgos de calidad.

Tabla 1 Ejemplos de puntos de riesgo y consecuencias de no controlarlos

PUNTO DE RIESGO	POSIBLES CONSECUENCIAS
Construcción de reportes de estados financieros	Investigaciones disciplinarias o fiscales
Ejercicios Planeación institucional	Incumplimiento de metas y objetivos
Seguimiento a la renovación de licencias de funcionamiento	Otorgamiento de licencias de funcionamiento sin el cumplimiento de todos los requisitos
Reporte de resultados de indicadores	Toma de decisiones sobre datos inoportunos e inexactos.
Diligenciamiento del Informe integral del niño, niña o adolescente.	Interrupción del proceso de adopción
Seguimiento y supervisión de contratos	Afectación de la imagen institucional

De manera integral para la gestión de los riesgos fiscales se contempla el siguiente listado de posibles puntos de fiscal el cual debe ser utilizado para la identificación y valoración de riesgos fiscales, atendiendo las particularidades, naturaleza, complejidad, recursos, usuarios o grupos de valor, portafolio de productos y servicios, sector en el cual se desenvuelva (contexto), así como otras condiciones específicas de cada entidad.

Tabla 2 Ejemplos punto de riesgos fiscales

PUNTOS DE RIESGO FISCAL *Actividad en la que potencialmente se origina el riesgo fiscal*	CIRCUNSTANCIA INMEDIATA *Situación **por la que** se presenta el riesgo*
Cumplimiento de las normas y obligaciones ante autoridades	Pago de multas, cláusulas penales o cualquier tipo de sanción
Cumplimiento de obligaciones	Pago de Intereses moratorios
Desplazamientos de los funcionarios y de los contratistas a lugares diferentes al domicilio de la entidad.	Pago de viáticos, honorarios o gastos de desplazamiento sin justificación o por encima de los valores establecidos normativamente
Liquidación de impuestos	Mayor valor pagado por concepto de impuestos
Operaciones, actas o actos en los que se reconocen saldos a favor de la entidad	Saldos o recursos a favor no cobrados
Custodiar de los bienes muebles de la entidad	Pérdida, extravío, hurto, robo o declaratoria de bienes faltantes pertenecientes a la Entidad
Avalúos a bienes inmuebles de la entidad	Error en los avalúos, afectando el valor de venta y/o negociación de un bien público
Custodiar de los bienes muebles de la entidad	Daño en bienes muebles de propiedad de la entidad
Suscripción de contratos cuyo objeto es o incluye la representación judicial o extrajudicial de la entidad	Valor pagado por concepto de honorarios de apoderado cuando ocurre vencimiento de términos en los procesos judiciales o cualquier otra omisión del apoderado
Pago de sentencias y conciliaciones	Intereses moratorios por pago tardío de sentencias y conciliaciones
Instrucción del Comité de Conciliación para iniciar acción de repetición	Caducidad de la acción de repetición o falencias en el ejercicio de esta acción, generando la imposibilidad de recuperar los recursos pagados por el Estado
Informe que acredite o anuncie la existencia de perjuicios generados a la entidad	Omisión en la obligación de impulsar acción judicial para cobrar clausula penal u otros perjuicios
Contratación de bienes o servicios	Contratación de bienes y servicios no relacionados con las funciones de la Entidad y que no generan utilidad
Contratación de bienes	Compra o inversión en bienes innecesarios o suntuosos

PUBLICA

PUNTOS DE RIESGO FISCAL *Actividad en la que potencialmente se origina el riesgo fiscal*	**CIRCUNSTANCIA INMEDIATA** *Situación **por la que** se presenta el riesgo*
Contratación de estudios y diseños	Estudios y diseños recibidos y pagados y que no cumplen condiciones de calidad
Suscripción de contratos de estudios y diseños	Estudios y diseños con amparo de calidad vencido al momento de contratar la obra y/o al momento de la ocurrencia
Suscripción de contratos	Sobrecostos en precios contractuales
Suscripción de contratos	Pagos efectuados a causa de riesgos previsibles que debieron ser asignados al contratista en la matriz de riesgos previsibles y no se le asignaron
Suscripción de contratos	No incluir en el contrato de seguros -amparo de bienes de la entidad- todos los bienes muebles e inmuebles de la entidad
Suscripción de contratos	No exigir garantía única de cumplimiento contractual
Suscripción de contratos respecto de los cuales la ley establece un cubrimiento mínimo en los amparos de la garantía única de cumplimiento	Exigir garantía única de cumplimiento contractual con un cubrimiento inferior al exigido por la ley
Pagos efectuados a contratistas	Pagar bienes, servicios u obras a pesar de no cumplir las condiciones de calidad.
Constancias de recibo a satisfacción de bienes, servicios u obras, firmadas por supervisor o interventor	Bienes, servicios u obras inconclusos, infuncionales y/o que no brindan utilidad o beneficio
Modificaciones contractuales firmadas	Modificaciones contractuales cuyas causas son imputables al contratista total o parcialmente y cuyos costos colaterales asume la Entidad contratante
Giros efectuados por concepto de anticipo contractual	Mal manejo o fallas en la legalización de anticipos, no amortización del anticipo
Giros efectuados por concepto de anticipo contractual	Rendimientos financieros de recursos de anticipo o de cualquier recurso público no devueltos al tesoro público
Reconocimiento y pago de desequilibrio contractual	Reconocimiento y pago de desequilibrio contractual por causa imputable a la Entidad
Firma de actas contractuales de recibo parcial o final	Errores o imprecisiones en las actas de recibo parcial o final
Firma de adiciones de ítems, actividades o productos no previstos (contratos adicionales)	Adición de ítem, actividad o producto no previsto sin estudio de mercado y/o con sobrecosto
Firma de adiciones de ítems, actividades o productos inicialmente previstos (adiciones)	Mayores cantidades reconocidas y pagadas con valores unitarios superiores al pactado en el contrato
Actos administrativos sancionatorios contractuales emitidos y ejecutoriados	Cuantificación errada de multa o clausula penal
Obras recibidas a satisfacción	Colapso o fallas en la estabilidad de la obra
Pagos finales efectuados a contratistas	Ejecución de un alcance inferior al contratado y pago total del contrato
Actas de recibo final a satisfacción firmadas	Disfuncionalidad de lo ejecutado
Contratos finalizados	Bienes, servicios u obras inconclusas y/o que no brindan utilidad o beneficio
Pagos efectuados a contratistas	Inadecuada deducción de impuestos, tasas o contribuciones al contratista
Pagos por concepto de comisión a éxito	Pago de comisiones a éxito sin debida justificación
Actas de liquidación suscritas	Suscripción de acta de liquidación con imprecisiones de fondo
Actas de liquidación suscritas	Suscripción de acta de liquidación sin relacionar las sanciones impuestas al contratista
Contratos finalizados en los que se contemplaba o requería liquidación.	Pérdida de competencia para liquidar por vencimiento del plazo legal, con saldos a favor de la Entidad
Actas de liquidación suscritas	Liquidación de mutuo acuerdo con recibo a satisfacción, habiendo imprecisiones o falsedades
Bienes u obras recibidas a satisfacción	Deterioro del bien u obra por indebido mantenimiento
Actas de recibo final a satisfacción firmadas	Suscripción de acta de recibo final con imprecisiones de fondo
Reintegro de saldos a favor de la entidad o pagos por parte de deudores	Reintegro de saldos a favor de la entidad sin indexación (reintegro sin actualización del dinero en el tiempo)

PUBLICA

PUNTOS DE RIESGO FISCAL *Actividad en la que potencialmente se origina el riesgo fiscal*	CIRCUNSTANCIA INMEDIATA *Situación **por la que** se presenta el riesgo*
Predios adquiridos	Adquisición de predios sin las especificaciones técnicas requeridas
Pérdida de tenencia de bienes de la entidad	Pérdida de la tenencia de bienes inmuebles de la Entidad
Pago de subsidios, transferencias o beneficios a particulares	Bases de datos con falencias de información que genera pagos de subsidios u otros beneficios sin el cumplimiento de requisitos y condiciones
Pago de subsidios, transferencias o beneficios a particulares	Pago de subsidio u otros beneficios a personas fallecidas
Pago de subsidios, transferencias o beneficios a particulares	Pago de subsidios u otros beneficios a personas que no tienen derecho a los mismos a la luz de requisitos de ley
Pago de subsidios, transferencias o beneficios a particulares	Pago de subsidios por encima del beneficio otorgado
Deudas a favor de la entidad	Vencimiento de plazos para la labor de cobro directo (persuasivo o coactivo) o judicial

2.1.7. Identificación Factores de Riesgos

Los factores de riesgo son aquellas fuentes a partir de las cuales se pueden generar los riesgos, en particular para la gestión del ICBF se tendrán en cuenta tres factores, el talento humano, los procesos y los eventos externos.

Tabla 3 Factores de Riesgos

FACTOR	DEFINICION	EJEMPLOS	
Talento Humano	Incluye lo referente a la actuación e interacción de las y los colaboradores de la entidad. Se analiza el posible dolo e intención frente a la corrupción.		Errores humanos
			Falta de competencia en una labor
			Posibles comportamientos no éticos de los colaboradores
Procesos	Eventos relacionados con errores en las actividades propias de la entidad.		Falta de procedimientos
			Errores de cálculo
			Falta de capacitación
			Deficiencia en los controles
Eventos Externos	Situaciones externas que afectan a la entidad.		Alta movilidad y dispersión de la población en el territorio.
			Alta migración de población vulnerable.
			Baja oferta de operadores en regiones apartadas

2.1.8. Descripción de Riesgo de Calidad y Fiscales

La descripción del riesgo debe contener información detallada que le permita a cualquier colaborador de la entidad entender fácilmente como se puede manifestar el riesgo, así como sus causas.

PÚBLICA

El riesgo fiscal se define como: "**Efecto dañoso sobre recursos públicos o bienes o intereses patrimoniales de naturaleza pública, a causa de un evento potencial.**"

Los elementos que componen la definición del riesgo fiscal son:

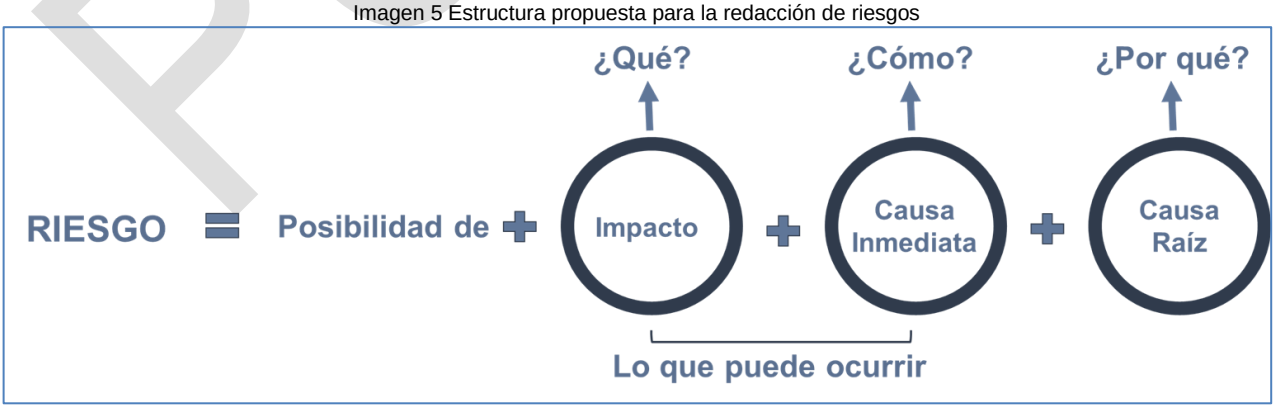
- **Efecto:** es el daño que se generaría sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de la entidad, en caso de ocurrir el evento potencial
- **Evento Potencial:** Son actos inciertos o incertidumbres, refiriéndonos a riesgo fiscal, se relaciona con una potencial acción u omisión que podría generar daño sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de la entidad. El evento potencial es equivalente a la causa raíz.

Para la identificación del riesgo fiscal es necesario establecer los **puntos de riesgo fiscal y las circunstancias Inmediatas**. Los puntos de riesgos son situaciones en las que potencialmente se genera riesgo fiscal, es decir, son aquellas actividades de administración, gestión, ordenación, ejecución, manejo, adquisición, planeación, conservación, custodia, explotación, enajenación, consumo, adjudicación, gasto, inversión y disposición de los bienes o recursos públicos, así como a la recaudación, manejo e inversión de sus rentas. Para las circunstancias inmediatas, se trata de aquella situación o actividad bajo la cual se presenta el riesgo, pero no constituyen la causa principal o básica - causa raíz- para que se presente el riesgo; es necesario resaltar que, por cada punto de riesgo fiscal, existen múltiples circunstancias inmediatas.

La causa raíz sería cualquier evento potencial (acción u omisión) que de presentarse provocaría un menoscabo, disminución, perjuicio, detrimento, pérdida o deterioro. La causa raíz o potencial hecho generador y el efecto dañoso (daño) guardan entre sí una relación de causa/efecto. En este sentido, la determinación de la causa raíz o potencial hecho generador se logra estableciendo la acción u omisión o acto lesivo del patrimonio estatal. Una adecuada gestión de riesgos fiscales exige que la identificación de causas sea especialmente objetiva y rigurosa, ya que los controles que se diseñen e implementen deben apuntarle atacar dichas causas, para así lograr prevenir la ocurrencia de daños fiscales.

De acuerdo con la metodología propuesta por el **Departamento Administrativo de la Función Pública** - **DAFP** se propone la siguiente estructura para la redacción de riesgos:

Imagen 5 Estructura propuesta para la redacción de riesgos



Fuente: Adaptado de la Guía para la administración del riesgo y diseño de controles en entidades públicas del **DAFP** por la Subdirección de Mejoramiento Organizacional del ICBF, 2022.

PÚBLICA

De acuerdo con la estructura tenemos:

- **Impacto:** Consecuencia de la materialización del riesgo para la entidad.
- **Causa Inmediata:** Circunstancias o situaciones más evidentes sobre las cuales se presenta el riesgo, las mismas no constituyen la causa principal o base para que se presente el riesgo.
- **Causa Raíz:** Causa principal o básica, corresponde a la razón por la cual se puede presentar el riesgo, es la base para la definición de controles en la etapa de valoración del riesgo. Se debe tener en cuenta que para un mismo riesgo pueden existir varias causas que pueden ser analizadas.

Ejemplo de redacción de un riesgo:

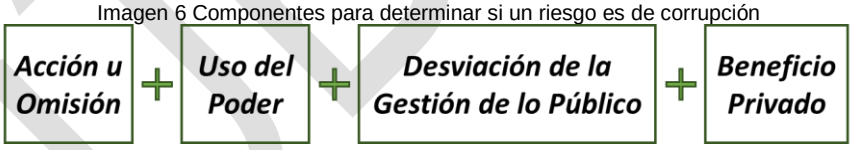
Tabla 4 Ejemplo redacción riesgo

"Posibilidad de afectación económica por multa y sanción del ente regulador debido a la adquisición de bienes y servicios sin el cumplimiento de los requisitos normativos"	***Impacto:*** *afectación económica por multa y sanción* ***Causa Inmediata:*** *a la adquisición de bienes y servicios* ***Causa Raíz:*** *cumplimiento de los requisitos normativos*

2.1.9. Descripción de Riesgo de Corrupción

Los riesgos de corrupción están definidos como la posibilidad de que, por acción u omisión se use el poder para desviar la gestión de lo público hacia un beneficio privado. En consecuencia, para describir un riesgo de corrupción deben concurrir los siguientes componentes:

Imagen 6 Componentes para determinar si un riesgo es de corrupción



Ejemplo descripción de un riesgo de corrupción:

Afectación del servicio público de bienestar familiar por otorgamiento de licencias de funcionamiento sin el cumplimiento del procedimiento, y del rigor técnico y administrativo en beneficio de los funcionarios y/o particulares.

Adicionalmente en la etapa de identificación de un riesgo de corrupción se debe realizar la identificación de sus causas y consecuencias.

Identificación de Causas: una vez se ha identificado un riesgo de corrupción se deben establecer aquellos medios, circunstancias o agentes generadores de riesgo que tienen la capacidad de originarlo.

Identificación de Consecuencias: Hacen referencias a los efectos de la ocurrencia del riesgo de corrupción para la entidad; generalmente se dan sobre las personas o los bienes, con incidencias

PÚBLICA

importantes tales como sanciones, pérdidas económicas, de información, de bienes, de imagen, de credibilidad y de confianza, entre otras.

2.1.10. Clasificación de Riesgos

Permite agrupar los riesgos identificados en categorías, lo que posibilita a los encargados de la gestión entender mejor la naturaleza del riesgo al que está expuesta la entidad.

Tabla 5 Clasificación de riesgos

Cumplimiento (ejecución o administración de procesos)	Son aquellos riesgos que surgen a partir de errores en la ejecución de los procesos y generan impacto sobre el cumplimiento de los objetivos.
Reputacional	Corresponde a riesgos cuya materialización afectaría la imagen, el buen nombre o la reputación de la entidad ante sus partes interesadas.
Económico	Riesgos que generan impacto negativo en los estados financieros de la entidad.
Corrupción	Son aquellos riesgos que se generan a partir de que por acción u omisión se use el poder para desviar la gestión de lo público hacia un beneficio privado.

Fuente: Adaptado de la Guía para la administración del riesgo y diseño de controles en entidades públicas del **DAFP** por la Subdirección de Mejoramiento Organizacional del ICBF, 2022.

2.1.11. Determina el nivel de aplicabilidad del riesgo

Una vez identificado el riesgo se debe establecer el o los niveles de la entidad a los que aplica, para esto es importante analizar donde se puede presentar un evento de riesgo materializado. A su vez la definición de aplicabilidad de los riesgos indicará los niveles en los cuales deben ser gestionados o tratados.

Los niveles definidos para la gestión de riesgos en el ICBF son:

- **Nivel Centro Zonal:** se refiere a la gestión en los Centros Zonales.
- **Nivel Regional:** hace referencia a las Direcciones Regionales y sus grupos de trabajo.
- **Nivel Nacional:** se refiere a las dependencias que de acuerdo con la estructura orgánica de la entidad hacen parte de la Sede de la Dirección General.

2.1.12. Valoración de Riesgos de Calidad

Consiste en establecer la probabilidad de ocurrencia del riesgo, así como la magnitud o nivel de impacto en la entidad de llegarse a materializar este, con el fin de determinar la zona de riesgo inicial o Riesgo inherente, para posteriormente determinar la zona de riesgo final o Riesgo Residual, el cual se establece una vez se analiza el riesgo inherente frente a los controles implementados para evitar su materialización y mitigar su impacto.

Etapas de la Valoración de Riesgos:

Análisis de Riesgo: En esta etapa se busca establecer la probabilidad de ocurrencia de un riesgo, así como su impacto de llegar a materializarse, con lo cual se determina la zona de riesgo inicial o riesgo inherente.

PÚBLICA

Evaluación de Riesgo: Consiste en establecer la zona de riesgo final o riesgo residual, la cual se obtiene una vez evaluado el riesgo inherente frente a los controles implementados para prevenir que el riesgo se materialice, así como para moderar el impacto de dicha materialización.

2.1.13. Análisis de Riesgo

Determinar la Probabilidad

La probabilidad de ocurrencia de un riesgo se entiende como la posibilidad de que se produzca una situación que afecte de forma negativa la consecución de los objetivos estratégicos y de procesos de la entidad. **De este modo la probabilidad inicial de un riesgo será determinada por el número de veces que se pasa por el punto de riesgo en un periodo de un año, o en otras palabras en número de veces que se realiza una actividad critica durante un año**.

Bajo esta lógica de calificación se elimina la subjetividad del análisis, ya que el resultado de este **depende de la frecuencia con la cual se realiza una actividad**, al mismo tiempo permite determinar un nivel de probabilidad más real para aquellos riesgos que nunca se han materializado. Como ejemplo, a continuación, se muestra una tabla con algunas actividades típicas de la entidad, las cuales están asociadas con la escala de probabilidad.

Tabla 6 Ejemplo de probabilidad de un riesgo

ACTIVIDAD CRITICA	FRECUENCIA DE LA ACTIVIDAD	PROBABILIDAD FRENTE AL RIESGO
Ejercicios de planeación estratégica	1 vez al año	Muy baja
Diligenciamiento del Informe integral del niño, niña o adolescente.	Varias veces al día	Muy Alta
Reporte de resultados de indicadores	Mensualmente	Baja

Fuente: Adaptado de la Guía para la administración del riesgo y diseño de controles en entidades públicas del **DAFP** por la Subdirección de Mejoramiento Organizacional del ICBF, 2022.

Nota: Para aquellas actividades que se realizan de manera continua se tienen en cuenta que 1 hora de funcionamiento equivale a 1 vez, un ejemplo de esto es el funcionamiento de las herramientas tecnológicas.

Teniendo en cuenta lo anterior, a continuación, se establecen los criterios para definir la probabilidad de un riesgo de calidad con base en un periodo de 1 año.

Tabla 7 Criterios de probabilidad riesgos de calidad y fiscal

PROBABILIDAD DE OCURRENCIA	FRECUENCIA DE LA ACTIVIDAD	PROBABILIDAD
Muy Baja	La actividad critica que conlleva el riesgo se ejecuta máximo 4 veces al año	20%
Baja	La actividad critica que conlleva el riesgo se ejecuta de 5 a 24 veces por año	40%
Media	La actividad critica que conlleva el riesgo se ejecuta de 25 a 110 veces por año	60%
Alta	La actividad critica que conlleva el riesgo se ejecuta de 111 a 365 veces por año	80%
Muy Alta	La actividad critica que conlleva el riesgo se ejecuta más de 365 veces por año	100%

Fuente: Adaptado de la Guía para la administración del riesgo y diseño de controles en entidades públicas del **DAFP** por la Subdirección de Mejoramiento Organizacional del ICBF, 2022.

PÚBLICA

Determinar el Impacto

Para determinar el nivel de impacto de un riesgo se tendrán en cuenta las 3 áreas de impacto definidas durante la etapa de identificación de riesgos, a saber, afectación *económica, reputacional y cumplimiento de los objetivos del proceso*, las cuales deberán ser valoradas teniendo en cuenta la escala determinada.

Es importante señalar que cuando se presenten varios impactos para un riesgo con diferentes niveles en su calificación, se tendrá en cuenta para determinar el nivel de riesgo inherente aquel que tenga la calificación más alta, por ejemplo: *para un riesgo identificado que cuenta con un impacto reputacional menor, un impacto por afectación económica moderado y un impacto al cumplimiento de objetivos del proceso mayor; se tomara el más alto, que en este caso correspondería con el cumplimiento de objetivos mayor*.

En consideración de lo anteriormente descrito, se define la escala para la valoración del impacto.

Tabla 8 Criterios de impacto riesgos de calidad y fiscal

NIVEL DE IMPACTO	AFECTACIÓN ECONÓMICA	REPUTACIONAL	CUMPLIMIENTO DE OBJETIVOS DEL PROCESO
Leve 20%	Afectación menor a 10 SMLMV	El riesgo afecta la imagen de algún área de la organización.	Sería imperceptible el impacto en el logro del objetivo.
Menor 40%	Entre 11 y 50 SMLMV	El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, de junta directiva y/o de proveedores.	Impactaría de manera mínima en el logro del objetivo.
Moderado 60%	Entre 51 y 100 SMLMV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos.	Impactaría moderadamente el logro del objetivo.
Mayor 80%	Entre 100 y 500 SMLMV	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal.	Impactaría en alto grado el objetivo del proceso.
Catastrófico 100%	Mayor a 500 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país.	No se lograría el objetivo del proceso

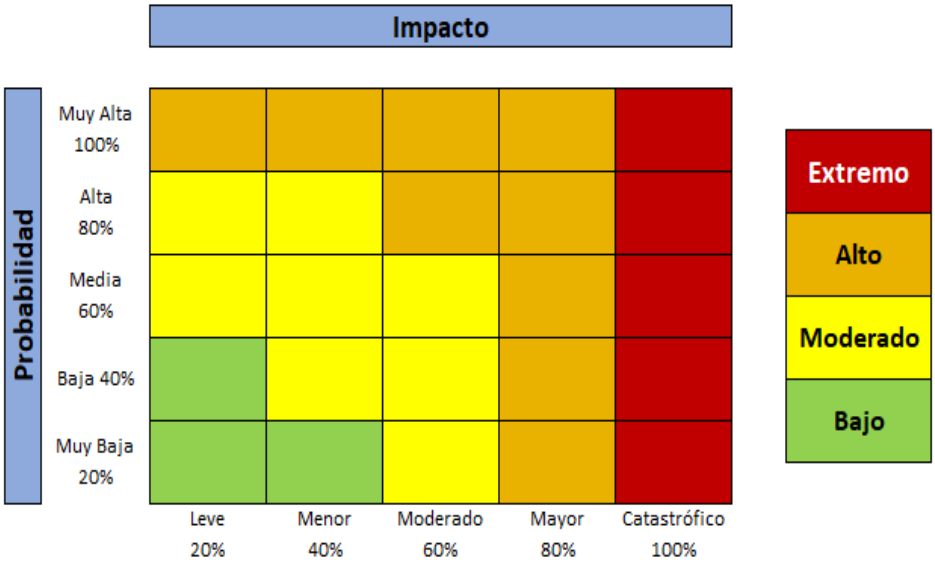
Fuente: Adaptado de la Guía para la administración del riesgo y diseño de controles en entidades públicas del **DAFP** por la Subdirección de Mejoramiento Organizacional del ICBF, 2022.

Nivel Riesgo Inherente

Se puede entender como la valoración del riesgo una vez establecida la probabilidad de ocurrencia, así como su nivel de impacto. Se puede determinar como la relación producto de la combinación de ambas variables, con lo cual se obtiene su ubicación en la matriz de calor, la cual determinará la zona de nivel de riesgo, que a su vez se asocia con la severidad de este.

PÚBLICA

Imagen 7 Mapa de Calor



Fuente: Adaptado de la Guía para la administración del riesgo y diseño de controles en entidades públicas del **DAFP** por la Subdirección de Mejoramiento Organizacional del ICBF, 2022.

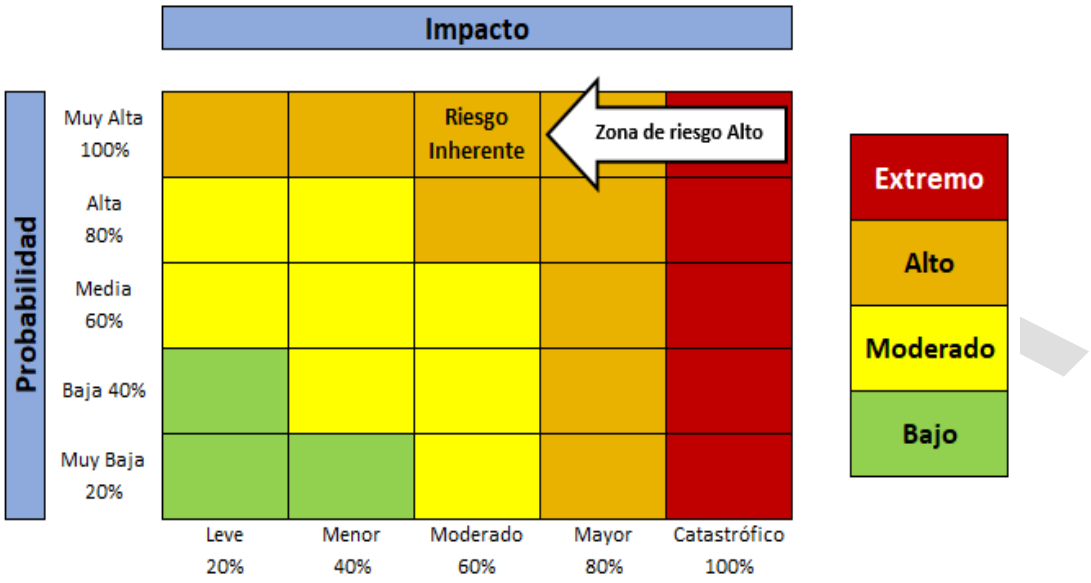
Ejemplo de análisis de un riesgo de calidad

Tabla 9 Ejemplo análisis riesgo de calidad

Riesgo: *Posibilidad de sanciones en materia civil, fiscal, penal o disciplinaria debido a faltas cometidas en el ejercicio de la supervisión, por deficiencias en el carácter jurídico, financiero o técnico, omitidas o transgredidas durante la etapa contractual y poscontractual.*	
Punto de Riesgo: *Ejercicios de supervisión.*	
Probabilidad: T*eniendo en cuenta que la probabilidad de un riesgo de calidad se mide a través de la frecuencia del punto de riesgo identificado, este riesgo tendrá una probabilidad muy alta dada la cantidad de contratos que se deben supervisar*.	**Muy Alta 100%**
Impacto: P*ara este ejemplo se determina que, si bien el riesgo podría generar impacto por afectación económica, así como reputacional, el impacto más alto se daría en el cumplimiento de objetivos, siendo este un impacto moderado.*	**Moderado 60%**

Teniendo en cuenta la información anterior, podemos determinar el nivel de riesgo inherente en el mapa de calor, para lo cual se ubicará en el espacio correspondiente a probabilidad “Muy Alta 100%” (primera fila de arriba hacia abajo), con un impacto “Moderado 60%” (tercera columna de izquierda a derecha), como se muestra a continuación:

Imagen 8 Determinación riesgo inherente mapa de calor



2.1.14. Evaluación de Riesgos de Calidad

Identificación de Controles

Un control se define como una medida o acción implementada para reducir o mitigar un riesgo. La identificación de controles se recomienda realizarse por cada uno de los riesgos, así mismo cada uno de los riesgos puede tener asociados varios controles.

Estructura para la Descripción de un Control

Para describir un control se propone la siguiente estructura en su redacción:

- **Responsable de ejecutar el control:** Es cargo o rol de quien ejecuta el control o garantiza su ejecución.
- **Acción:** Indica la acción que se realiza al ejecutar el control
- **Complemento:** Todos los detalles necesarios para entender claramente el propósito del control.

Tabla 10 Ejemplo descripción de control

El profesional de contratación verifica el componente jurídico y contractual, cuando existan observaciones técnicas o financieras.	***Responsable:*** *Profesional de Contratación.*
	Acción: *Verificar componente jurídico y contractual.*
	Complemento: *Cuando existan observaciones técnicas o financieras.*

Caracterización de Controles

Una vez descrito el control, para poder analizarlo, se debe completar la información de este mediante la asignación de unas características establecidas, las cuales se dividen en dos grupos de acuerdo

con su naturaleza, los atributos de eficiencia, sobre los cuales se calificará el control, y los atributos informativos que permitirán conocer el entorno del control y complementar la información que permita hacer un análisis cualitativo de este. Los atributos informativos no tienen incidencia en la calificación de un control.

Clasificación de acuerdo con los atributos de eficiencia: Para clasificar los controles según sus atributos de eficiencia deben ser analizados a través de 2 tipologías; en primer lugar, debe analizarse en qué fase del ciclo de procesos se aplica el control, esto permite determinar si el control es preventivo, detectivo o correctivo (tipo de control); la segunda tipología indica la forma como se ejecuta o implementa el control, si es manual o automático (forma de implementación).

Acorde con lo anterior se tienen las siguientes clasificaciones de acuerdo con el tipo de control:

- **Preventivo:** Se aplican en la entrada de los procesos (antes de que se realice la actividad crítica que genera el riesgo) y se enfocan en las causas del riesgo, de tal forma que previenen su materialización con lo cual reducen la probabilidad de ocurrencia.

- **Detectivo:** Se ejecuta durante la realización del proceso (mientras se realiza la actividad crítica que genera el riesgo) de forma que al detectar una desviación no permite continuar, con lo cual se generan reprocesos. Los controles detectivos se enfocan en evitar que el riesgo se materialice al no permitir que se avance con una actividad, estos reducen la probabilidad de ocurrencia.

- **Correctivo:** Un control es correctivo cuando se ejecuta a partir de las salidas del proceso (después de realizar la actividad crítica que produce el riesgo), es decir que aplican una vez el riesgo se ha materializado, y su propósito es reducir el impacto negativo que genera dicha materialización.

Imagen 9 Flujo de procesos y tipos de controles

Fuente: Adaptado de la Guía para la administración del riesgo y diseño de controles en entidades públicas del **DAFP** por la Subdirección de Mejoramiento Organizacional del ICBF, 2022.

De acuerdo con la forma como se implementa o ejecuta el control

- **Automático:** Corresponde a controles que son realizados por sistemas y/o aplicativos sin que intervengan personas en su realización.

- **Manual:** Aquellos ejecutados por personas, con lo cual tienen implícito el error humano.

Valoración de Controles

Una vez definidos los controles, para determinar su peso en la mitigación del riesgo asociado se deben tener en cuenta sus atributos de eficiencia, es decir el tipo de control y la forma como se ejecuta o implementa, con lo que se obtendrá la calificación del riesgo residual. A continuación, se relaciona el peso de cada atributo:

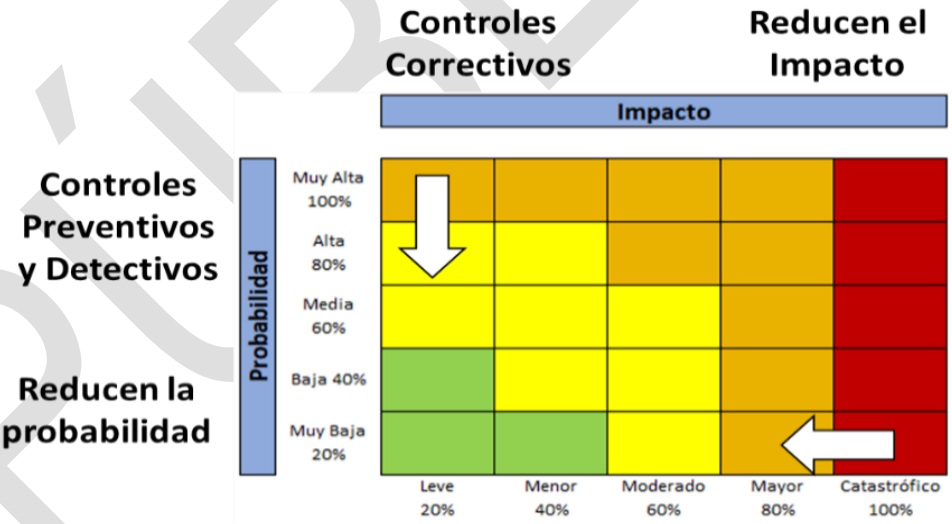
Tabla 11 Ponderación atributos de eficiencia de controles

CARACTERÍSTICAS		PESO
Tipo	Preventivo	25%
	Detectivo	15%
	Correctivo	10%
Implementación	Automático	25%
	Manual	15%

Fuente: Adaptado de la Guía para la administración del riesgo y diseño de controles en entidades públicas del **DAFP** por la Subdirección de Mejoramiento Organizacional del ICBF, 2022.

De acuerdo con el tipo de control se establecerá el eje de la matriz de riesgos (probabilidad o impacto) en el cual se moverá. Si el control reduce el impacto, la ubicación del riesgo se moverá a la izquierda, si por el contrario reduce la probabilidad, se moverá hacia abajo, en la siguiente imagen se muestra la aplicación de lo anterior.

Imagen 10 Movimiento de los riesgos en la matriz de calor acorde al tipo de control



Fuente: Adaptado de la Guía para la administración del riesgo y diseño de controles en entidades públicas del **DAFP** por la Subdirección de Mejoramiento Organizacional del ICBF, 2022.

Clasificación de acuerdo con los atributos informativos: Con estas características se busca complementar la información de los controles estableciendo la formalidad del control para conocer su entorno, de acuerdo con lo anterior se podrá establecer, si está documentado, su frecuencia de ejecución y si se cuenta o no con evidencias de esta.

PÚBLICA

Tabla 12 Atributos informativos controles de riesgo

ATRIBUTO	CLASIFICACIÓN	DESCRIPCIÓN
Documentación	**Documentado**	El control se encuentra descrito en un documento del proceso (procedimientos, guías, manuales, operativos, lineamientos, etc.)
	Sin documentar	El control si bien se ejecuta no se encuentra descrito en ningún documento.
Frecuencia	**Continua**	El control se ejecuta cada vez que se realiza la actividad crítica que genera el riesgo.
	Aleatoria	El control se ejecuta de manera aleatoria a la realización de la actividad que genera el riesgo.
Evidencia	**Con registro**	Cuando se ejecuta el control se genera un registro que permite evidenciar su aplicación.
	Sin registro	Cuando se ejecuta el control no se genera un registro y por lo tanto no se puede evidenciar su aplicación.

El siguiente ejemplo sirve para entender mejor cómo se hace la caracterización y se establece la valoración de un grupo de controles

Tabla 13 Ejemplo valoración controles riesgos calidad

DESCRIPCIÓN DEL CONTROL	CARACTERISTICAS DEL CONTROL			PESO
Control 1	**Tipo**	Preventivo		
El o la profesional de contratación verifica el componente jurídico y contractual, cuando existan observaciones técnicas o financieras.		Detectivo	X	15%
		Correctivo		
	Implementación	Automático		
		Manual	X	15%
	Documentación	Documentado	X	-
		Sin Documentar		
	Frecuencia	Continua		
		Aleatoria	X	-
	Evidencia	Con registro	X	-
		Sin Registro		
Total, Valoración Control 1				**30%**
Control 2	**Tipo**	Preventivo		
Las o los abogados del Grupo Jurídico en las Direcciones Regionales realizan seguimiento y verificación periódica al cumplimiento de las liquidaciones y cierres en la Regional.		Detectivo	X	15%
		Correctivo		
	Implementación	Automático		
		Manual	X	15%
	Documentación	Documentado	X	-
		Sin Documentar		
	Frecuencia	Continua		
		Aleatoria	X	-
	Evidencia	Con registro	X	-
		Sin Registro		
Total, Valoración Control 2				**30%**

Fuente: Adaptado de la Guía para la administración del riesgo y diseño de controles en entidades públicas del **DAFP** por la Subdirección de Mejoramiento Organizacional del ICBF, 2022.

PÚBLICA

Nivel de Riesgo Residual

El nivel de riesgo residual es la calificación del riesgo que se obtiene una vez aplicados los controles, la cual dependerá de la valoración de los controles asociados a este. Para calcular el riesgo residual se deberá calcular de forma acumulativa, es decir, se calcula el valor de probabilidad o impacto de acuerdo con el peso del primer control y sobre el resultado se aplicará el segundo control, así sucesivamente dependiendo del número de controles.

A continuación, se desarrolla un ejemplo de lo anterior, para dar claridad de la metodología para determinar el nivel de riesgo residual.

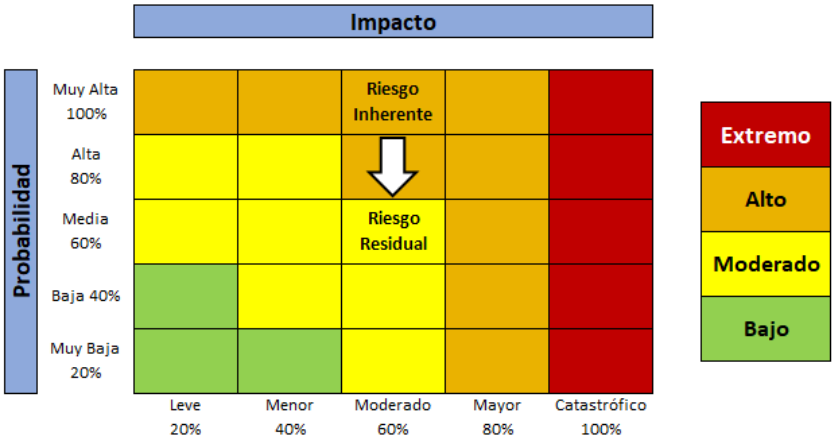
Tabla 14 Aplicación de controles para calcular el riesgo residual

RIESGO	CALIFICACIÓN RIESGO INHERENTE		VALORACIÓN CONTROLES		CALCULOS
Posibilidad de afectación económica por multa y sanción del ente regulador debido a la adquisición de bienes y servicios sin el cumplimiento de los requisitos normativos	Probabilidad Inherente	100%	Valoración Control 1 Detectivo	30%	100% * 30% = 30% 100% - 30% = 70%
	Valor Probabilidad tras aplicar control 1	70%	Valoración Control 2 Detectivo	30%	70% * 30% = 21% 70% - 21% = 49%
	Probabilidad Residual				**49%**
	Impacto Inherente	60%	N/A	N/A	N/A
	Impacto Residual				**60%**

Fuente: Adaptado de la Guía para la administración del riesgo y diseño de controles en entidades públicas del **DAFP** por la Subdirección de Mejoramiento Organizacional del ICBF, 2022.

Con los valores de probabilidad e impacto residuales, se procede a ubicar el riesgo en el mapa de calor teniendo en cuenta las mismas indicaciones que en la etapa de análisis. Como se observa a continuación una vez aplicados los controles el riesgo bajó dos niveles en su probabilidad, quedando en una zona de riesgo Moderado.

Imagen 11 Riesgo residual mapa de calor



PÚBLICA

2.1.15 Valoración Riesgos de Corrupción

Al igual que para los riesgos de calidad, para valorar los riesgos de corrupción se deberán desarrollar dos etapas:

Análisis de Riesgo: Incluye la definición de la probabilidad, el impacto y el nivel de riesgo inherente.

Evaluación de Riesgo: En la cual se definirán los controles, así como su valoración, de tal manera que se pueda calcular el nivel de riesgo residual.

Análisis de Riesgo

Determinar la Probabilidad en los Riesgos de Corrupción

Teniendo en cuenta la naturaleza particular de los riesgos de corrupción, su probabilidad se establecerá basados en la frecuencia o factibilidad de su ocurrencia, entendiendo como frecuencia el número de eventos en un periodo determinado, es decir eventos de materialización del riesgo o situaciones relacionadas al riesgo; de otra parte la factibilidad implica el análisis de factores internos y/o externos que puedan propiciar la materialización del riesgo, y el análisis de la posibilidad de ocurrencia de un evento de materialización de riesgo, lo que no necesariamente supone que se haya presentado.

El análisis de probabilidad para los riesgos de corrupción deberá realizarse teniendo en cuenta la siguiente tabla:

Tabla 15 Escala de probabilidad para riesgos de corrupción

NIVEL	PROBABILIDAD DE OCURRENCIA	DESCRIPCIÓN	FRECUENCIA
5	Casi seguro	Se espera que el evento ocurra en la mayoría de las circunstancias.	Más de 1 vez al año.
4	Probable	Es viable que el evento ocurra en la mayoría de las circunstancias.	Al menos 1 vez en el último año.
3	Posible	El evento podrá ocurrir en algún momento.	Al menos 1 vez en los últimos 2 años.
2	Improbable	El evento puede ocurrir en algún momento.	Al menos 1 vez en los últimos 5 años.
1	Rara vez	El evento puede ocurrir solo en circunstancias excepcionales (poco comunes o anormales)	No se ha presentado en los últimos 5 años.

Fuente: Guía para la administración del riesgo y diseño de controles en entidades públicas del **DAFP**.

Determinar el Impacto en Riesgos de Corrupción

Cuando se requiere determinar el impacto de un riesgo de corrupción es necesario realizar un análisis especial, el cual consiste en responder de manera afirmativa o negativa las 19 preguntas que se relacionan en la siguiente tabla.

PUBLICA

Tabla 16 Criterios para la calificación del impacto en riesgos de corrupción

#	Pregunta: Si el riesgo de corrupción se materializara podría …
1	¿Afectar al grupo de funcionarios del proceso?
2	¿Afectar el cumplimiento de metas y objetivos de la dependencia?
3	¿Afectar el cumplimiento de misión de la Entidad?
4	¿Afectar el cumplimiento de la misión del sector al que pertenece la Entidad?
5	¿Generar pérdida de confianza de la Entidad, afectando su reputación?
6	¿Generar pérdida de recursos económicos?
7	¿Afectar la generación de los productos o la prestación de servicios?
8	¿Dar lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien o servicios o los recursos públicos?
9	¿Generar pérdida de información de la Entidad?
10	¿Generar intervención de los órganos de control, de la Fiscalía, u otro ente?
11	¿Dar lugar a procesos sancionatorios?
12	¿Dar lugar a procesos disciplinarios?
13	¿Dar lugar a procesos fiscales?
14	¿Dar lugar a procesos penales?
15	¿Generar pérdida de credibilidad del sector?
16	¿Ocasionar lesiones físicas o pérdida de vidas humanas?
17	¿Afectar la imagen regional?
18	¿Afectar la imagen nacional?
19	¿Generar daño ambiental?

Fuente: Guía para la administración del riesgo y diseño de controles en entidades públicas del **DAFP**.

Una vez son respondidas las preguntas, se determina el nivel de impacto del riesgo de corrupción dependiendo del número de preguntas cuya respuesta sea afirmativa, como se muestra en siguiente tabla.

Tabla 17 Nivel de impacto en riesgos de corrupción

Número de Respuestas Afirmativas	Nivel de Impacto	Descripción
De **1** a **5** respuestas afirmativas	**Moderado**	Afectación parcial al proceso o más procesos Genera medianas consecuencias para la entidad.
De **6** a **11** respuestas afirmativas	**Mayor**	Impacto negativo de la Entidad Genera altas consecuencias para la entidad.
De **12** a **19** respuestas afirmativas	**Catastrófico**	Consecuencias desastrosas sobre el sector Genera consecuencias desastrosas para la entidad.

Fuente: Guía para la administración del riesgo y diseño de controles en entidades públicas del **DAFP**.

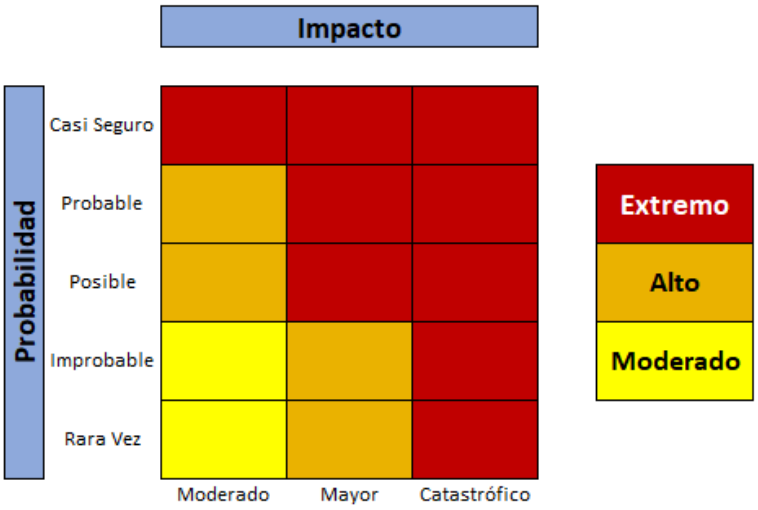
Como se puede observar cuando se trata de riesgo de corrupción el nivel impacto siempre será significativo, por lo que para este tipo de riesgos los niveles de impacto leve y menor no aplican.

Nivel Riesgo Inherente en los Riesgos de Corrupción

Se puede entender como la valoración del riesgo una vez establecida la probabilidad de ocurrencia, así como su nivel de impacto. Se puede determinar como la relación producto de la combinación de ambas variables, con lo cual se obtiene una ubicación en la matriz de calor que, dependiendo de su ubicación dentro de una de las 3 zonas definidas se obtendrá la clasificación del nivel de riesgo, el cual está asociado a la severidad de este. A continuación, se presentan el mapa de calor.

PUBLICA

Imagen 12 Mapa de calor riesgos de corrupción



Fuente: Guía para la administración del riesgo y diseño de controles en entidades públicas del **DAFP**.

Ejemplo de análisis de un riesgo de corrupción

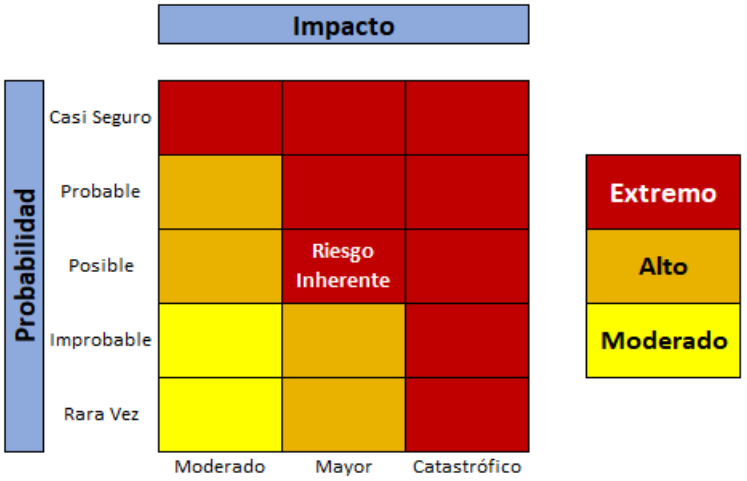
Tabla 18 Ejemplo análisis riesgo de corrupción

Riesgo: Afectación del servicio público de bienestar familiar por otorgamiento de licencias de funcionamiento sin el cumplimiento del procedimiento, y del rigor técnico y administrativo en beneficio de los funcionarios y/o particulares.	
Probabilidad: Se estableció que el nivel de probabilidad del riesgo es “Posible”, lo cual nos indica que el evento podrá ocurrir en algún momento, o que ha ocurrido al menos una vez en los últimos 2 años.	**Posible**
Impacto: Producto del análisis del riesgo se determinó que era afirmativa la respuesta a las preguntas 1, 3, 5, 7, 10, 11, 12, 14, 15, 17 y 18, obteniendo así un nivel de impacto “Mayor”.	**Mayor**

Teniendo en cuenta la información anterior podemos determinar el nivel de riesgo inherente en el mapa de calor, para lo cual se ubicará en el espacio correspondiente a probabilidad “Posible” (tercera fila de arriba hacia abajo), con un impacto “Mayor” (segunda columna de izquierda a derecha), como se muestra a continuación:

PÚBLICA

Imagen 13 Determinación del riesgo inherente en el mapa de calor para un riesgo de corrupción



Evaluación de Riesgos de Corrupción

Identificación de Controles

Para la identificación y descripción de los controles asociados a los riesgos de corrupción se propone la estructura descrita en la Guía para la administración del riesgo y el diseño de controles en entidades públicas V4 de 2018, la cual indica que se conforma por el diseño del control y la ejecución de estos. A continuación, se describen los criterios de diseño y de ejecución de los controles.

Imagen 14 Estructura para describir un control

Tabla 19 Ejemplo descripción de control riesgo de corrupción

Los abogados de la Dirección de Contratación verifican mensualmente los requisitos para la suscripción, modificación o liquidación del contrato o convenio, a través del control de legalidad en cumplimiento a los puntos de control establecidos en cada uno de los procedimientos, dejando como evidencia los correos electrónicos. En caso de identificar novedades, se remiten por correo electrónico al área técnica para su subsanación.	**Responsable:** Los abogados de la Dirección de Contratación.
	Periodicidad: Mensual**.**
	Propósito: Cumplimiento de requisitos para suscripción, modificación o liquidación de contratos.
	Cómo se realiza: a través del control de legalidad en cumplimiento a los puntos de control establecidos en cada uno de los procedimientos
	Observaciones y/o Desviaciones: Se remiten observaciones mediante correo electrónico
	Evidencia: Correos electrónicos**.**

Caracterización de Controles Asociados a Riesgo de Corrupción: Para determinar los controles asociados a los riesgos de corrupción se deben tener en cuenta los siguientes criterios, sobre los cuales se calificarán, de forma que se establezca su peso en la gestión del riesgo.

Tabla 20 Criterios de diseño controles asociados a riesgos de corrupción

CRITERIO	DESCRIPCIÓN
Responsable	Corresponde al cargo dentro de la entidad bajo cuya responsabilidad esta ejecutar o garantizar la ejecución del control. Para establecer la idoneidad de este responsable es indispensable analizar las siguientes pautas: - Funciones de control asignadas y debidamente documentadas. - Segregación de funciones, es decir quien aplica o ejerce el control debe ser un funcionario diferente a quien realiza la actividad a controlar (este ítem tiene peso sobre la calificación del control). - El responsable debe contar con el conocimiento adecuado para ejecutar el control. Adicionalmente es importante mencionar que es el líder o responsable del proceso en el marco del cual se ejecuta el control, quien debe asignar al responsable de la ejecución del control teniendo en cuenta los parámetros mencionados.
Periodicidad	Es el espacio de tiempo en el cual se realiza o ejecuta el control, la cual debe estar debidamente definida y ser consistente y oportuna para evitar el riesgo.
Propósito	Es el objeto con el cual se realiza el control (para qué), el cual debe estar orientado a prevenir las causas que generan el riesgo (verificar, validar, conciliar, compara, revisar, cotejar), o a detectar una posible materialización de manera que se realicen los ajustes pertinentes para evitarla.
Cómo se realiza la actividad de control	El control debe indicar el cómo se realiza, de tal forma que se pueda evaluar si la fuente u origen de la información que sirve para ejecutarlo es confiable para evitar la materialización del riesgo.
Qué pasa con las observaciones o desviaciones	El control indicara la manera de actuar ante la identificación de observaciones o desviaciones cuando se ejecuta. Es importante definir la manera de actuar ante el incumplimiento de alguno de los parámetros de la actividad que se está controlando.
Evidencia de Ejecución	Es el registro de la ejecución del control, la cual permite hacer seguimiento y validación de los resultados de la aplicación del control, y evaluar el cumplimiento de esta de acuerdo con los parámetros establecidos.

Fuente: Guía para la administración del riesgo y diseño de controles en entidades públicas del **DAFP**.

Valoración de Controles Asociados a Riesgos de Corrupción

Una vez los controles son definidos de acuerdo con los criterios de diseño deben ser calificados acorde con la siguiente tabla:

Tabla 21 Valoración criterios de diseño controles asociados a riesgos de corrupción

Criterio de Evaluación	Opción de respuesta al criterio de evaluación	Peso en la evaluación del diseño del control
Responsable	Asignado	15
	No Asignado	0
Segregación y autoridad del responsable	Adecuado	15
	Inadecuado	0
Periodicidad	Oportuna	15
	Inoportuna	0
Propósito	Prevenir	15
	Detectar	10
	No es un control	0
¿Cómo se realiza la actividad de control?	Confiable	15
	No confiable	0
	Se identifica y se gestionan para subsanar la observación	15

PÚBLICA

Criterio de Evaluación	Opción de respuesta al criterio de evaluación	Peso en la evaluación del diseño del control
¿Qué pasa con las observaciones o desviaciones?	No se identifica ni se gestionan para subsanar la observación	0
Evidencia de la ejecución	Completa	10
	Incompleta	5
	No existe	0

Fuente: Guía para la administración del riesgo y diseño de controles en entidades públicas del **DAFP**.

La calificación del diseño de un control se calcula como la sumatoria del peso asignado a cada uno de los criterios de diseño. Dependiendo del resultado numérico de la calificación de los controles se puede establecer si un control es fuerte, moderado o débil en su diseño.

Tabla 22 Calificación de diseño de control

Calificación del Diseño del Control	Rango de Calificación Cuantitativa del Control
Fuerte	Calificación entre 96 y 100
Moderado	Calificación entre 86 y 95
Débil	Calificación entre 0 y 85

Fuente: Guía para la administración del riesgo y diseño de controles en entidades públicas del **DAFP**.

Una vez establecida la calificación del diseño de un control es necesario medir la ejecución de este, de tal forma que se pueda determinar si el control se aplica en el transcurso normal de las actividades de acuerdo con los criterios establecidos.

Para la medir la ejecución de un control es importante tener en cuenta los siguientes aspectos:

- Verificar que los criterios de diseño se encuentran validados y preferiblemente documentados.
- Validar que en el desarrollo de las actividades del proceso los controles se ejecutan de acuerdo con los criterios definidos en el diseño.
- Contar con evidencia de la ejecución del control.

Para medir la ejecución de los controles están definidas tres categorías, las cuales se describen a continuación:

Tabla 23 Criterios de ejecución de controles asociados a riesgos de corrupción

Criterios de Evaluación de la Ejecución	Descripción
Fuerte	El control se ejecuta de manera consistente por parte del responsable.
Moderado	El control se ejecuta algunas veces por parte del responsable.
Débil	El control no se ejecuta por parte del responsable.

Fuente: Guía para la administración del riesgo y diseño de controles en entidades públicas del **DAFP**.

Después de determinar las calificaciones del diseño y la ejecución de un control, se podrá establecer la calificación de la solidez de este como una relación de las dos primeras, cuyo resultado indicará

PÚBLICA

si el control implementado mitiga el riesgo de corrupción asociado. La relación entre la calificación del diseño y la de ejecución se establece en la siguiente tabla:

Tabla 24 Criterios de calificación solidez individual de controles asociados a riesgos de corrupción

Calificación Diseño	Calificación Ejecución	Solidez individual de cada control *Fuerte: 100* *Moderado: 50* *Débil:0*
Fuerte **Calificación entre 96 y 100**	Fuerte (siempre se ejecuta)	fuerte + fuerte = fuerte (100)
	Moderado (algunas veces)	fuerte + moderado = moderado (50)
	Débil (no se ejecuta)	fuerte + débil = débil (0)
Moderado **Calificación entre 86 y 95**	Fuerte (siempre se ejecuta)	moderado + fuerte = moderado (50)
	Moderado (algunas veces)	moderado + moderado = moderado (50)
	Débil (no se ejecuta)	moderado + débil = débil (0)
Débil **Calificación entre 0 y 85**	Fuerte (siempre se ejecuta)	débil + fuerte = débil (0)
	Moderado (algunas veces)	débil + moderado = débil (0)
	Débil (no se ejecuta)	débil + débil = débil (0)

Fuente: Guía para la administración del riesgo y diseño de controles en entidades públicas del **DAFP**.

Para entender mejor como se evalúa un riesgo de acuerdo con su diseño y ejecución, se desarrolla el siguiente ejemplo:

Tabla 25 Ejemplo calificación solides de un control asociado a un riesgo de corrupción

CONTROL	CRITERIOS DE DISEÑO				EJECUCIÓN
Los profesionales de la Oficina de Aseguramiento a la Calidad revisan y avalan periódicamente las licencias de funcionamiento previamente a los procesos contractuales.	**Responsable**	Asignado	X	15	**FUERTE** El control se ejecuta de manera consistente por parte del responsable
		No Asignado			
	Segregación y autoridad del responsable	Adecuado	X	15	
		Inadecuado			
	Periodicidad	Oportuna	X	15	
		Inoportuna			
	Propósito	Prevenir	X	15	
		Detectar			
		No es un control			
	Cómo se realiza la actividad de control	Confiable	X	15	
		No confiable			
	Qué pasa con las observaciones o desviaciones	Se identifica y se gestionan para subsanar la observación	X	15	
		No se identifica y se gestionan para subsanar la observación			
	Evidencia de la ejecución	Completa	X	10	
		Incompleta			
		No existe			
	Puntaje Total Criterios de Diseño		**100**		

De acuerdo con el resultado de la calificación de los criterios de diseño y ejecución del control y según la tabla 23, tenemos que la solidez individual del control es fuerte (100).

PÚBLICO

Nivel de Riesgo Residual de los Riesgos de Corrupción

Para determinar el nivel de riesgo residual de un riesgo de corrupción es necesario realizar primero la calificación de la solidez del conjunto de controles asociados a este, la cual se entiende como el promedio de las calificaciones individuales de la solidez de cada control.

Para el análisis del resultado de la solidez del conjunto de controles asociados a un riesgo de corrupción se tendrán los elementos relacionados en la siguiente tabla:

Tabla 26 Criterios de calificación solidez conjunto de controles asociados a riesgos de corrupción

Solidez Conjunto de Controles	Rangos de Calificación según promedio de los Controles	Descripción
Fuerte	El promedio de la solidez individual de cada control al sumarlos y ponderarlos es igual a 100.	El conjunto de controles mitiga el riesgo asociado y no requieren de acciones adicionales para su tratamiento.
Moderado	El promedio de la solidez individual de cada control al sumarlos y ponderarlos la calificación está entre 50 y 99	El conjunto de controles mitiga parcialmente el riesgo asociado. Para su tratamiento se requiere tomar acciones adicionales, las cuales serán incluidas en el plan de tratamiento de riesgos.
Débil	El promedio de la solidez individual de cada control al sumarlos y ponderarlos la calificación es menor a 50.	El conjunto de controles no mitiga el riesgo asociado. Se requiere estudiar la viabilidad de estos controles y tomar acciones a fin de tratar adecuadamente el riesgo o implementar nuevos controles.

Fuente: Guía para la administración del riesgo y diseño de controles en entidades públicas del **DAFP**.

De acuerdo con el resultado de la calificación de la solidez del conjunto de controles asociados a un riesgo de corrupción, el líder o responsable de proceso en la Sede de la Dirección General podrá definir acciones que fortalezcan el conjunto de controles, las cuales pueden incluir la implementación de nuevos controles.

Una vez evaluada la solidez del grupo de controles asociados a un riesgo de corrupción, para determinar el nivel de riesgo residual se debe tomar la ubicación del riesgo inherente en el mapa de calor y desplazarla de acuerdo con la tabla relacionada a continuación, así se establecerá gráficamente el nivel de riesgo residual.

Tabla 27 Solidez del Conjunto de Controles

Solidez del conjunto de los controles.	Controles ayudan a disminuir la probabilidad	# Filas en la matriz de riesgo que se desplaza en el eje de la probabilidad
Fuerte	Directamente	**2**
Moderado	Directamente	**1**

Fuente: Guía para la administración del riesgo y diseño de controles en entidades públicas del **DAFP**.

Nota 1: Si la solidez del conjunto de los controles es débil, este no disminuirá ningún cuadrante de probabilidad asociado al riesgo.

Nota 2: Tratándose de riesgos de corrupción únicamente hay disminución de probabilidad. Es decir, para el impacto no opera el desplazamiento.

PUBLICA

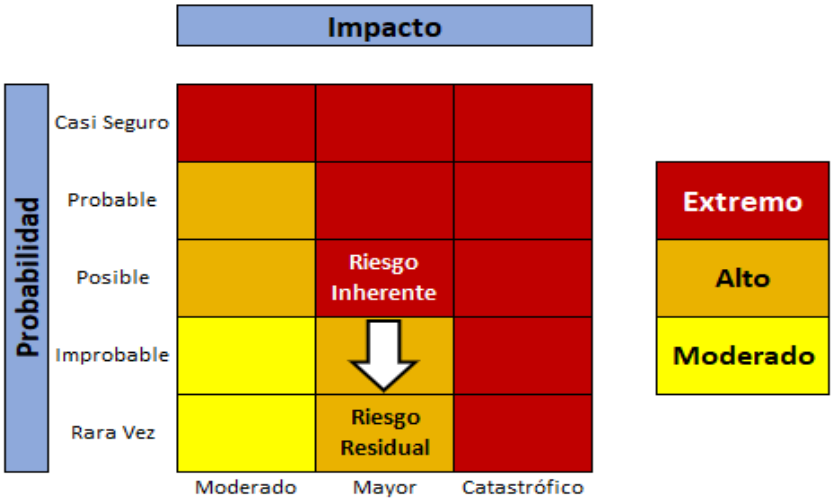
Para entender cómo se define el nivel de riesgo residual de un riesgo de corrupción tomaremos el ejemplo anterior donde se estableció lo siguiente:

Tabla 28 Información continuación ejemplo riesgo residual para riesgos de corrupción

Riesgo: Afectación del servicio público de bienestar familiar por otorgamiento de licencias de funcionamiento sin el cumplimiento del procedimiento, y del rigor técnico y administrativo en beneficio de los funcionarios y/o particulares.
Probabilidad: Posible
Impacto: Mayor
Control: Los profesionales de la Oficina de Aseguramiento a la Calidad revisan y avalan periódicamente las licencias de funcionamiento previamente a los procesos contractuales.
Calificación Diseño Control: Fuerte 100
Calificación Ejecución Control: Fuerte. El control se ejecuta de manera consistente por parte del responsable
Solidez Individual Control: Fuerte 100
Solidez Conjunto de Controles: como en este caso solo se estableció un control la solidez del conjunto de controles será el valor de la solidez individual del control.

Con base en la información del cuadro anterior se puede concluir que el nivel de probabilidad del riesgo una vez aplicado el control se reducirá en 2, pasando de una zona de riesgo Extremo a Alto como se muestra en la imagen 15.

Imagen 15 Riesgo residual mapa de calor corrupción



Tratamiento de Riesgos

Cuando la calificación del riesgo residual sea moderado, alto o extremo el líder o responsable de proceso debe implementar estrategias que permitan combatir los riesgos evitando así que se materialice. Lo anterior no quiere decir que cuando un riesgo se encuentre en nivel bajo no pueda ser tratado.

Para realizar el tratamiento de riesgos se tendrán tres estrategias posibles, que serán evitar, transferir o mitigar el riesgo.

Evitar: Consiste en que posteriormente a determinar el nivel de riesgo residual, se decide eliminar la actividad crítica que provoca el riesgo, con lo cual se eliminaría o evitaría el riesgo. Sin embargo, mientras no se realicen los ajustes pertinentes al proceso y la actividad siga vigente, el riesgo deberá ser gestionado a través de alguna de las otras estrategias de tratamiento.

Transferir: Consiste en trasladar el riesgo a un tercero, bien sea tercerizando el proceso o a través de una póliza de seguro. Esta estrategia aplicará únicamente para aquellos riesgos cuyo impacto sea económico, en tal caso se deberá hacer un análisis basado en los otros tipos de impacto para definir si el riesgo persiste en la entidad.

Mitigar: Consiste en implementar acciones para reducir el nivel de riesgo. En el marco de esta estrategia, se pueden establecer dos escenarios siempre enmarcados en un plan de tratamiento que contemple: actividades definidas, responsables, fechas de inicio y fin, periodicidad (para actividades que se repitan durante un periodo de tiempo), evidencias y seguimiento, lo cuales pueden ser:

- **Implementar nuevos controles:** Como su nombre lo indica esta estrategia consiste en generar nuevos controles dentro del proceso que contribuyan a mejorar la calificación del riesgo residual, atacando la probabilidad de ocurrencia del riesgo o su impacto.

- **Realizar actividades complementarias de mitigación de riesgos:** Consiste en la realización de actividades que contribuyan a evitar la materialización del riesgo, que pueden ser, seguimientos, actividades de fortalecimiento al recurso humano, verificaciones, entre otras. Es importante recordar que estas actividades deben estar en el marco de un plan de trabajo y contar con las características antes mencionadas.

2.1.16. Monitoreo y Revisión

La entidad debe asegurar el logro de sus objetivos, anticipándose a los eventos negativos relacionados con la gestión de riesgos al interior de sus procesos. Se determinan las responsabilidades de los participantes de la gestión de riesgos de la entidad, esto proporciona aseguramiento de la gestión y previene la materialización de los riesgos. A continuación, se mencionan los grupos de responsabilidades y las funciones que desarrollan bajo el esquema de líneas de defensa determinado en el Sistema de Control Interno de la siguiente manera:

LÍNEA ESTRATEGICA: Compuesta por la Dirección General y el Comité Institucional de Coordinación de Control Interno, quienes deben definir el marco general para la gestión del riesgo y el control, así como supervisar su cumplimiento y realizar seguimiento a los resultados de las evaluaciones realizadas por la Oficina de Control Interno y la Dirección de Planeación y Control de Gestión

PRIMERA LÍNEA DE DEFENSA: Conformada por Líderes o Responsables de Proceso, Secretaria General, Subdirección General, Directores, Subdirectores y Jefes de Oficina SDG, Directores Regionales, Coordinadores de Centro Zonal, Coordinadores de Grupos Internos y colaboradores en general, quienes desarrollan e implementan acciones de control y gestión de riesgos a través de su

PÚBLICA

identificación, análisis, valoración, seguimiento y acciones de mejora para el cumplimiento de los objetivos institucionales y de los procesos incluyendo las siguientes actividades:

- Revisar los cambios en el direccionamiento estratégico o en el contexto que puedan generar nuevos riesgos o modificar los que ya se tienen identificados en cada uno de sus procesos.
- Revisar el adecuado diseño y ejecución de los controles establecidos para la mitigación de los riesgos.
- Revisar y reportar, los eventos de riesgos que se han materializado en la entidad, incluyendo los riesgos de corrupción, así como las causas que dieron origen a esos eventos de riesgos materializados y definir los planes de acción correspondientes y realizar su seguimiento.
- Revisar y hacer seguimiento al cumplimiento de los controles y los planes de tratamiento definidos para la vigencia con relación a la gestión de riesgos.

SEGUNDA LÍNEA DE DEFENSA: Conformada por la Dirección de Planeación y Control de Gestión con el apoyo de la Subdirección de Mejoramiento Organizacional y los Líderes de eje del SIGE asisten y guían la gestión de los riesgos que pueden afectar el cumplimiento de los objetivos institucionales y de los procesos, incluyendo los riesgos de corrupción y fiscales.

- Asistir y apoyar la identificación, análisis, evaluación de controles y tratamiento de los riesgos, y realizar monitoreo al cumplimiento de las etapas de la gestión de riesgos.
- Monitorear el diseño y aplicación de los controles para la mitigación de los riesgos que se han establecido por parte de la primera línea de defensa y realizar las recomendaciones para su fortalecimiento.
- Monitorear las acciones correctivas de los riesgos materializados, con el fin de que se tomen medidas oportunas y eficaces para evitar en lo posible que se vuelva a presentar.

TERCERA LÍNEA DE DEFENSA: Representada por la Oficina de Control Interno, hace seguimiento y revisa de manera independiente y objetiva el cumplimiento de las diferentes etapas de la gestión de riesgos en los procesos en la entidad, incluyendo los riesgos de corrupción.

- Revisar la aplicación y la efectividad de los controles, planes de tratamiento y actividades de monitoreo vinculadas a la gestión de riesgos de la entidad
- Seguimiento a la materialización de riesgos en la entidad, así como al cumplimiento de los planes de acción de las acciones correctivas definidas por cada proceso.
- Adelantar seguimiento a los Riesgos de Corrupción.
- Alertar sobre la probabilidad de riesgo de fraude o corrupción en las áreas auditadas

Control Fiscal Interno

Adicional a lo anterior también es pertinente mencionar y definir el **Control Fiscal Interno** el cual es el primer nivel para la vigilancia fiscal de los recursos públicos y para la prevención de riesgos fiscales y defensa del patrimonio público. El Control Fiscal Interno, hace parte del Sistema de Control Interno y es responsabilidad de todos los servidores públicos y de los particulares que administran recursos, bienes, e intereses patrimoniales de naturaleza pública y de las líneas de defensa, en lo que corresponde a cada una de ellas. El Control fiscal interno es evaluado por la contraloría, siendo dicha evaluación determinante para el fenecimiento de la cuenta.

PUBLICA

2.1.17. Monitoreo y Seguimiento Riesgos de Corrupción

Los líderes y/o responsables de procesos de la entidad en la Sede de la Dirección General, Direcciones Regionales y Centros Zonales con sus grupos de trabajo deben realizar el seguimiento y reporte del cumplimiento de los planes de tratamiento definidos para gestionar los riesgos de corrupción identificados en su proceso, y disponer las evidencias de estos en el repositorio destinado por la Subdirección de Mejoramiento Organizacional, quien con base en el reporte realiza el monitoreo. Adicionalmente a lo anterior, la Oficina de Control Interno debe adelantar seguimiento al Mapa de Riesgos de Corrupción teniendo en cuenta las siguientes fechas:

- **Primer seguimiento:** Con corte al 30 de abril. En esa medida, la publicación deberá surtirse dentro de los diez (10) primeros días hábiles del mes de mayo.
- **Segundo seguimiento:** Con corte al 31 de agosto. La publicación deberá surtirse dentro de los diez (10) primeros días hábiles del mes de septiembre.
- **Tercer seguimiento:** Con corte al 31 de diciembre. La publicación deberá surtirse dentro de los diez (10) primeros días hábiles del mes de enero.

El seguimiento adelantado por la Oficina de Control Interno deberá ser publicado en la página web de la entidad, y deberá contener el resultado de las siguientes actividades:

- Verificar la publicación del Mapa de Riesgos de Corrupción en la página web de la entidad.
- Seguimiento a la gestión del riesgo.
- Revisión de los riesgos y su evolución.
- Revisar que los controles sean efectivos, le apunten al riesgo y estén funcionando en forma adecuada

2.1.18. Comunicación y Consulta

Esta actividad se desarrolla de manera transversal en las diferentes etapas de la gestión del riesgo en el ICBF, con el fin de generar un proceso participativo de la gestión del riesgo. Se refiere al conocimiento que deben tener quienes participan en la gestión del riesgo, con el fin de lograr que las decisiones en la materia se tomen con base en información pertinente y actualizada, para lo cual se estructuran y realizan divulgaciones y socializaciones para los colaboradores de la gestión. Además, se cuenta con diferentes momentos para que interactúen los responsables de las actividades y se pueda desarrollar adecuadamente todas las etapas. Cada vez que se realiza la identificación, análisis y evaluación de riesgos en los procesos, los responsables de procesos en el nivel nacional, regional y zonal deben comunicar, socializar y retroalimentar, a los actores de la gestión en todos los niveles.

La entidad cuenta con una política de riesgos la cual es aprobada por el Comité Institucional de Coordinación de Control Interno que abarca la presente guía de gestión de riesgos, la cual se divulga vía correo electrónico y se publica en la intranet y página web de la entidad. Cada vigencia, se realizan mesas de trabajo en la Sede de la Dirección General, donde se identifican y analizan los riesgos de cada uno de los procesos incluyendo los de corrupción; en estas mesas los líderes y/o responsables de procesos previamente realizan un análisis de insumos determinados los cuales

PÚBLICA

incluyen los resultados de los cuestionarios de validación de riesgos de calidad y corrupción aplicados al nivel regional.

3. GESTIÓN DE PELIGROS DE SEGURIDAD Y SALUD EN EL TRABAJO

La identificación de peligros, valoración de riesgos y determinación de controles, es el punto de partida para la implementación, sostenibilidad y mejora del Sistema de Gestión de Seguridad y Salud en el Trabajo-SGSST y del Plan Estratégico de Seguridad Vial - PESV, ya que constituye el diagnóstico inicial de las condiciones o situaciones que puedan causar afectación a las y los colaboradores o al instituto, el propósito de la metodología establecida en este capítulo es entender los peligros que se pueden generar en el desarrollo de los procesos y actividades con el fin de poder determinar las medidas de intervención que se van a implementar para establecer y mantener la seguridad y salud de sus colaboradores y otras partes interesadas.

Así mismo, conforme al decreto 1072 de 2015 del Ministerio de Trabajo (Artículos 2.4.6.8, 2.2.4.6.15 Parágrafo 1, 2.2.4.6.23 y 2.2.4.6.24), la norma ISO 45001:2018 (Numeral 6.1.2) y la Resolución 40595 del 2022 (paso 6. Caracterización, evaluación y control de riesgos), la entidad deberá realizar el análisis y la identificación de peligros de manera continua y proactiva, evaluación y valoración de los riesgos, y determinación de controles que prevengan daños en la salud de los colaboradores y/o contratistas, instalaciones, vehículos y equipos.

Por lo anterior, el instituto adoptó la metodología de la Guía Técnica Colombiana GTC 45:2012 y Resolución 40595 del 2022 del Ministerio de Transporte estableciendo las herramientas necesarias para que los profesionales del grupo de desarrollo del talento humano de la Dirección de Gestión Humana, profesional del Grupo Administrativo, Gestión Humana o Gestión de Soporte, y colaboradores de la entidad, puedan realizar su implementación de manera clara y permanente.

3.1. Objetivos Específicos

- Determinar la metodología para la identificación de peligros, valoración de riesgos y determinación de los controles de Seguridad y Salud en el Trabajo y Plan Estratégico de Seguridad Vial – PESV asociados a las y los colaboradores, procesos, actividades e infraestructura del ICBF.
- Identificar los peligros y valorar los riesgos presentes A nivel nacional, Regional y Zonal, procesos y actividades del ICBF a los cuales están expuestos las y los colaboradores para la prevención de incidentes, accidentes y enfermedades laborales.
- Analizar las consecuencias y probabilidad antes de que los peligros identificados se materialicen.
- Priorizar los peligros identificados en la matriz para implementar sistemas de control encaminados a su mitigación y mejora continua.
- Comprobar si las medidas de control existentes en el lugar de trabajo son efectivas para reducir los riesgos.
- Evaluar la eficacia de los controles implementados e identificar la necesidad de modificar o introducir nuevos controles.
- Incluir a los representantes de los colaboradores y partes interesadas en la identificación de peligros, valoración de riesgos y determinación de controles.

PÚBLICA

- Sensibilizar a los colaboradores sobre la importancia de informar las situaciones peligrosas y condiciones inseguras, de manera que puedan ponerse en práctica medidas preventivas y puedan tomarse acciones correctivas.

3.2. Políticas operacionales para la identificación de peligros, valoración de riesgos y determinación de los controles de Seguridad y Salud en el Trabajo y Plan Estratégico de Seguridad Vial

a) Realizar anualmente la identificación de peligros, valoración de riesgos y determinación de los controles de seguridad y salud en el trabajo y del Plan Estratégico de Seguridad Vial, así mismo, validar la matriz cada vez que se incorporen o modifiquen los procesos, se presenten cambios en los requisitos legales aplicables y/o se ejecuten nuevos proyectos, actividades o cambios en la naturaleza física u operacional, y producto de ello se generen nuevos peligros o modificaciones en su valoración, y/o cada vez que ocurra un siniestro vial en el cual resulte involucrado un vehículo de la Entidad o puesto al servicio de ella y a consecuencia del mismo se causen fatalidades o lesiones; o cuando se presente un siniestro vial de un miembro de la comunidad del ICBF al interior o en su entorno, o cuando se presenten cambios en las actividades relacionadas con el transporte.

b) Para la identificación de peligros y valoración de riesgos se deben considerar las condiciones de operación normal, así como las actividades esporádicas o no rutinarias, los incidentes y accidentes de trabajo (leves, graves o mortales), enfermedades laborales, conceptos médico ocupacionales, recomendaciones médicas laborales, situaciones de emergencia que ocurran o puedan ocurrir dentro de la realización de las actividades, y consultas con los colaboradores y partes interesadas, análisis de las causas de los siniestros viales, diagnóstico de seguridad vial, teniendo en cuenta instalaciones, vehículos, equipos, elementos y sustancias que se emplean.

c) Para la identificación de condiciones inseguras que puedan generar potencial de peligro, se tomarán los resultados obtenidos en las inspecciones y reportes de condiciones inseguras, teniendo en cuenta que su frecuencia se determina en el programa de inspecciones de seguridad, inspecciones de puestos de trabajo, e inspección preoperacional de vehículo y equipos.

d) Incluir en los informes de gestión trimestral la actualización y las modificaciones realizadas en la matriz de peligros, valoración de riesgos y determinación de controles, de acuerdo con la ocurrencia de incidentes y accidentes de trabajo, enfermedad laboral (leves, graves o mortales) y sinestros viales, así mismo identificar cambios como materialización de peligros, modificación en controles y ajustes en la evaluación del riesgo.

e) Realizar seguimiento a los controles establecidos en la matriz de Identificación de Peligros, Valoración de Riesgos y Determinación de Controles según la periodicidad establecida en el Plan de Trabajo anual del SGSST, así como documentar el avance de estos e incluir el soporte en cada caso en la carpeta destinada para tal fin. En caso de considerar necesario la inclusión de algún peligro o información adicional, gestionar la misma con el Profesional del Grupo de Desarrollo del Talento Humano de la Dirección de Gestión Humana.

PÚBLICA

f) Generar acciones de mejora acorde con los resultados de la implementación de controles.

g) Generar acciones de gestión del cambio frente a la Entidad, operaciones, actividades, Sistema de Gestión Seguridad y Salud en el Trabajo y Plan Estratégico de Seguridad Vial.

h) Tener en cuenta los resultados de las evaluaciones de los factores de riesgo psicosocial con el fin de identificar, evaluar e incluir en las medidas de intervención.

i) Tener en cuenta los resultados e informes producto de las mediciones higiénicas realizadas, identificando si se requiere modificar la valoración del riesgo.

j) Deberán mantenerse las diferentes versiones de actualización de la identificación de peligros y valoración de riesgos, con el fin de poder ver su progreso y trazabilidad, dando cumplimiento al Decreto 1072 de 2015 del Ministerio de Trabajo.

3.3. Responsabilidad y Autoridad

La responsabilidad y autoridad del presente capítulo se encuentra a cargo del Director de Gestión Humana como encargado del Sistema de Seguridad y Salud en el Trabajo, de los Directores de las Regionales, Profesional del Grupo de Desarrollo del Talento Humano de la Dirección de Gestión Humana, Profesional del Grupo Administrativo, Gestión Humana o Gestión de Soporte, Comité Paritario de Seguridad y Salud en el Trabajo - COPASST y los colaboradores de la entidad.

El Comité de Seguridad Vial realizará el seguimiento a los controles en lo relacionado al peligro de tránsito.

3.4. Metodología

Para la identificación de peligros, valoración de riesgos y determinación de controles, se deberá realizar a través de la herramienta Suite Visión empresarial – SVE, manteniendo la metodología GTC 45:2012 y la Resolución 40595 del 2022 del Ministerio de Transporte.

3.4.1. Identificación de las instalaciones: Se deben identificar las sedes, áreas, y las actividades que se realizan, tanto rutinarias como no rutinarias. En esta identificación de actividades se deben tener en cuenta las labores realizadas por el personal de planta, contratista, pasantes y/o visitantes.

Nota: Para seguridad vial se tendrán en cuenta los siguientes roles: peatones/pasajeros y conductores de vehículos automotores y no automotores.

3.4.2. Cada regional debe contar con un código de identificación del requisito el cual se compondrá de la siguiente forma:

- Amazonas: MPR AMAZ 011
- Antioquia: MPR ANTI 011
- Arauca: MPR ARAU 011
- Atlántico: MPR ATLA 011

PÚBLICA

- Bogotá: MPR BOGO 011

Imagen 16 SVE

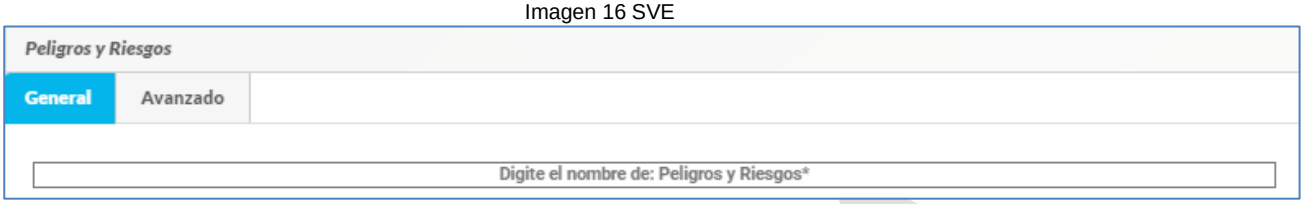
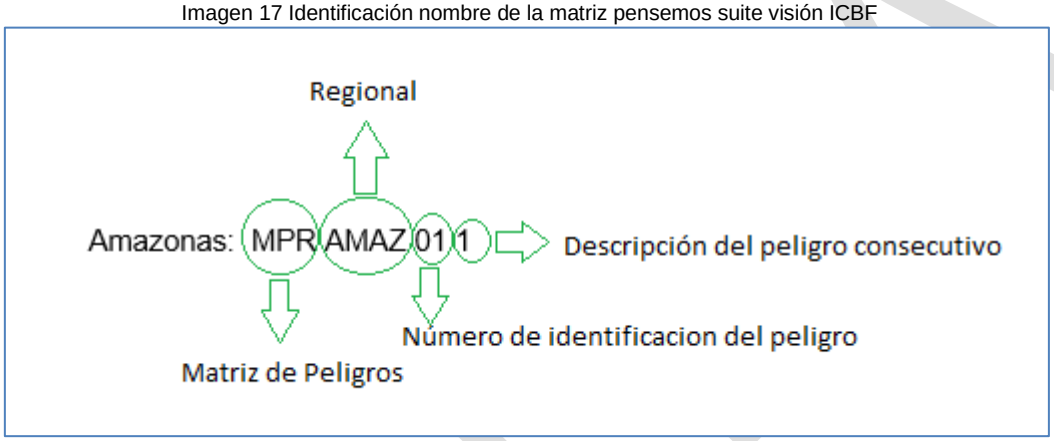


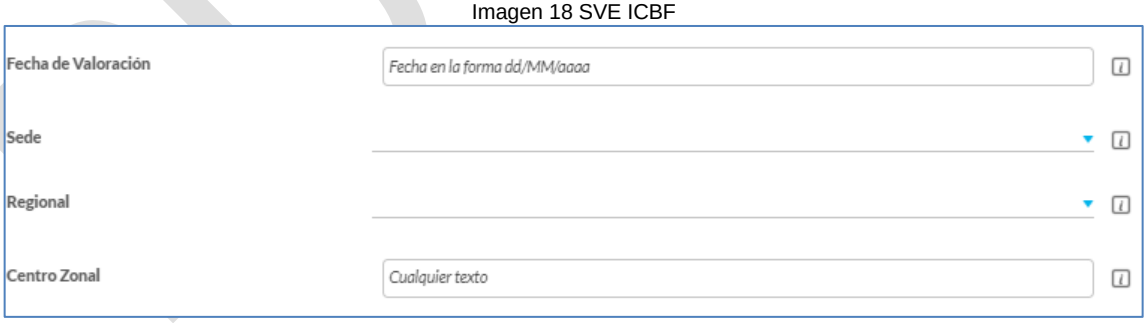
Imagen 17 Identificación nombre de la matriz pensemos suite visión ICBF



3.4.3. Identificación de Peligros y Valoración de Riesgos: Se utilizará el aplicativo de Suite Visión Empresarial para la identificación de peligros, valoración de riesgos y determinación de los controles.

a. Datos de Identificación de la Matriz: Incluir la información correspondiente, y fecha en la que se realizó la identificación de peligros y valoración de los riesgos, Sede (Si aplica), Regional y/o Centro Zonal:

Imagen 18 SVE ICBF



b. Identificación, clasificación y descripción de peligros: Se realiza con el fin de entender los peligros que se pueden generar en el desarrollo de las actividades de la Entidad, instalaciones, colaboradores, vehículos, equipos, procedimientos, y valorar los riesgos derivados de los mismos para determinar posteriormente las medidas de control necesarias**.**

c. Clasificación: Seleccionar en la lista despegable el peligro identificado.

Tabla 29 Clasificación Peligro

Clasificación	**01 Biológico**
	02 Eléctrico
	03 Locativo
	04 Natural
	05 Psicosocial
	06 Transito
	07 Biomecánico
	08 Físico
	09 Químico
	10 Mecánico
	11 Publico
	12 Alturas

La identificación de peligros se realiza teniendo en cuenta la infraestructura e instalaciones y/o entorno, el diseño de las áreas de trabajo, los equipos, materiales, condiciones físicas del lugar de trabajo, vehículos, sustancias que se emplean (*específicamente al área donde se está desarrollando la actividad ya sea rutinaria o no rutinaria*), factores humanos y la organización del trabajo, posibles situaciones de emergencia potenciales y sus causas, que puedan ocurrir dentro de la realización de las actividades o instalaciones, reportes de condiciones inseguras, incidentes y accidentes de trabajo, enfermedades laborales, diagnósticos médico-ocupacionales, permiso de trabajo en alturas y análisis de trabajo seguro (ATS), siniestros viales, y si aplica entrevista verbal con los colaboradores, así como inspecciones de seguridad, acciones de mejora, los cambios en el conocimiento y la información sobre los peligros.

Nota: Se deben identificar los peligros que se originan fuera del lugar de trabajo con capacidad de afectar adversamente la salud y la seguridad de los colaboradores que están bajo el control de la organización en el lugar de trabajo y los peligros generados en la vecindad y/o del lugar de trabajo.

d. Descripción: Identificar la lista despegable denominada *"Descripción de Peligro*", las características del peligro identificado, aquí se pueden elegir varias descripciones siempre y cuando estas tengan la misma valoración y aplique a las mismas actividades seleccionadas, de lo contrario se deberá identificar en otra fila.

e. Proceso: Identificar y seleccionar en la lista despegable el o los procesos a los cuales se va a realizar valoración de riesgos, de acuerdo con el peligro identificado.

f. Descripción de la actividad: Labor que forma parte de un proceso del ICBF, y puede ser rutinaria o no rutinaria. Luego de identificar el peligro, su descripción y el proceso, clasifíquelas de acuerdo con las opciones establecidas.

- Actividad rutinaria: Actividad que forma parte de un proceso del ICBF, se ha planificado y se ha estandarizado.
- Actividad no rutinaria: Actividad sin planificar ni estandarizar dentro de un proceso del Instituto o la actividad que se determine como no rutinaria por su baja frecuencia de ejecución.

PUBLICA

g. Efectos posibles: Se realiza la identificación de aquellos eventos, sucesos o demás aspectos que pueden provocar una situación que genere la materialización del peligro, se deben tener en cuenta las consecuencias a corto plazo (incidentes y accidentes de trabajo) y largo plazo (enfermedades laborales), además de daños leves (molestias e irritación y/o enfermedad temporal que produce malestar, lesiones superficiales, heridas de poca profundidad contusiones), daños moderados (enfermedades que causan incapacidad temporal, laceraciones, heridas profundas, quemaduras de primer grado, conmoción cerebral, esguinces graves, fracturas de huesos cortos) y daños extremos (enfermedades agudas o crónicas, lesiones que generen amputaciones, fracturas de huesos largos, traumas, quemaduras de segundo o tercer grado). Igualmente se deben tener en cuenta preguntas tales como:

- ¿Cómo puede ser afectado el colaborador o la parte interesada expuesta?
- ¿Cuál es el daño que le(s) puede ocurrir?

h. Controles existentes: Se debe identificar los controles existentes para cada uno de los peligros identificados y clasificarlos en:

- Fuente: Donde el peligro se origina.
- Medio: Entorno en el cual se desarrolla o transmite el peligro.
- Trabajador: Persona afectada o posiblemente afectada por el peligro.

i. Evaluación del riesgo: Se hace para determinar la probabilidad de que ocurran eventos específicos y la magnitud de sus consecuencias, mediante el uso de información disponible. Para la evaluación del riesgo se implementa la metodología de la GTC 45:2012, en el Formato Matriz de identificación de peligros, valoración de riesgos y determinación de controles, se encuentran las listas desplegables para la valoración del riego, a excepción del peligro de tránsito:
El nivel de riesgo se calcula como (NR):

$$\boldsymbol{NR = NP \times NC}$$

En donde:
NP= Nivel de probabilidad
NC= Nivel de consecuencia

A su vez para determinar el (NP) se requiere:

$$\boldsymbol{NP = ND \times NE}$$

En donde:
ND= Nivel de deficiencia
NE= Nivel de exposición

Para determinar estos parámetros se tiene en cuenta las siguientes tablas, con sus respectivas calificaciones tomadas de la GTC 45.

PÚBLICA

Tabla 30 Determinación del Nivel de Deficiencia

DETERMINACIÓN DEL NIVEL DE DEFICIENCIA (ND)		
NIVEL DE DEFICIENCIA	**VALOR DEL ND**	**SIGNIFICADO**
Muy Alto (MA)	10	Se ha(n) detectado peligro(s) que determina(n) como posible la generación de incidentes o consecuencias muy significativas, o la eficacia del conjunto de medidas preventivas existentes respecto al riesgo es nula o no existe, o ambos.
Alto (A)	6	Se ha(n) detectado algún(os) peligro(s) que pueden dar lugar a consecuencias significativa(s), o la eficacia del conjunto de medidas preventivas existentes es baja, o ambos.
Medio (M)	2	Se han detectado peligros que pueden dar lugar a consecuencias poco significativas o de menor importancia o la eficacia del conjunto de medidas preventivas existentes es moderada o ambos
Bajo (B)	No se asigna valor	No se ha detectado consecuencia alguna, o la eficacia del conjunto de medidas preventivas existentes es alta o ambos. El riesgo está controlado

El nivel de deficiencia para los peligros provenientes de los agentes higiénicos se calcula teniendo en cuenta los resultados de las mediciones realizadas, para los casos en los que aplica (Peligro psicosocial, Físico, Químico, entre otros), y lo indicado en la siguiente tabla:

Tabla 31 Parámetros para Determinar el Nivel de Deficiencia de los Peligros Higiénicos

FÍSICOS	
ILUMINACIÓN	
MUY ALTO	Ausencia de luz natural o artificial
ALTO	Deficiencia de luz natural o artificial con sombras evidentes y dificultad para leer
MEDIO	Percepción de algunas sombras al ejecutar una actividad.
BAJO	Ausencia de sombras
RUIDO	
MUY ALTO	No escuchar una conversación a una intensidad normal a una distancia menos de 50 cm.
ALTO	Escuchar la conversación a una distancia de 1 m a una intensidad normal.
MEDIO	Escuchar la conversación a una distancia de 2 m a una intensidad normal.
BAJO	No hay dificultad para escuchar una conversación normal a una intensidad normal a más de 2 m.
RADIACIONES IONIZANTES	
MUY ALTO	Exposición frecuente (una o más veces por jornada o turno).
ALTO	Exposición regular (una o más veces en la semana)
MEDIO	Ocasionalmente y/o vecindad.
BAJO	Rara vez casi nunca sucede la exposición.
Nota: Cuando se tenga sospecha de que hay exposición a un agente altamente radiactivo en la labor desempeñada, necesariamente tendrá que hacerse mediciones para determinar el nivel de exposición en referencia al TLV correspondiente (Véase Anexo E), sin dejar de valorarlo cualitativamente mientras obtiene las mediciones, teniendo en cuenta criterios como riesgos presentes en trabajos similares, información de entes especializados, etc.	
RADIACIONES NO IONIZANTES	
MUY ALTO	Ocho horas (8) o más de exposición por jornada o turno
ALTO	Entre seis (6) horas y (8) ocho horas por jornada o turno
MEDIO	Entre dos (2) y seis (6) horas por jornada o turno

PUBLICA

BAJO	Menos de dos (2) horas por jornada o turno
TEMPERATURAS EXTREMAS	
MUY ALTO	Percepción subjetiva de calor o frío en forma inmediata en el sitio.
ALTO	Percepción subjetiva de calor o frío luego de permanecer 5 min en el sitio
MEDIO	Percepción de algún Disconfort con la temperatura luego de permanecer 15 min.
BAJO	Sensación de confort térmico
VIBRACIONES	
MUY ALTO	Percibir notoriamente vibraciones en el puesto de trabajo
ALTO	Percibir sensiblemente vibraciones en el puesto de trabajo
MEDIO	Percibir moderadamente vibraciones en el puesto de trabajo
BAJO	Existencia de vibraciones que no son percibidas
BIOLOGICOS	
VIRUS, BACTERIAS, HONGOS Y OTROS	
MUY ALTO	Provocan una enfermedad grave y constituye un serio peligro para los trabajadores. Su riesgo de propagación es elevado y no se conoce tratamiento eficaz en la actualidad.
ALTO	Pueden provocar una enfermedad grave y constituir un serio peligro para los trabajadores. Su riesgo de propagación es probable y generalmente existe tratamiento eficaz.
MEDIO	Pueden causar una enfermedad y constituir un peligro para los trabajadores. Su riesgo de propagación es poco probable y generalmente existe tratamiento eficaz.
BAJO	Poco probable que cause una enfermedad. No hay riesgo de propagación y no se necesita tratamiento
BIOMECANICOS	
POSTURA	
MUY ALTO	Posturas con un riesgo extremo de lesión musculoesquelética. Deben tomarse medidas correctivas inmediatamente.
ALTO	Posturas de trabajo con riesgo probable de lesión. Se deben modificar las condiciones de trabajo tan pronto como sea posible.
MEDIO	Posturas con riesgo moderado de lesión musculoesquelética sobre las que se precisa una modificación, aunque no inmediata.
BAJO	Posturas que se consideran normales, sin riesgo de lesiones musculoesqueléticas, y en las que no es necesaria ninguna acción
MOVIMIENTOS REPETITIVOS	
MUY ALTO	Actividad que exige movimientos rápidos y continuos de los miembros superiores, a un ritmo difícil de mantener (ciclos de trabajo menores a 30 s o 1 min, o concentración de movimientos que utiliza pocos músculos durante más del 50 % del tiempo de trabajo)
ALTO	Actividad que exige movimientos rápidos y continuos de los miembros superiores, con la posibilidad de realizar pausas ocasionales (ciclos de trabajo menores a 30 segundos o 1 min, o concentración de movimientos que utiliza pocos músculos durante más del 50 % del tiempo de trabajo).
MEDIO	Actividad que exige movimientos lentos y continuos de los miembros superiores, con la posibilidad de realizar pausas cortas.
BAJO	Actividad que no exige el uso de los miembros superiores, o es breve y entrecortada por largos periodos de pausa.
ESFUERZO	
MUY ALTO	Actividad intensa en donde el esfuerzo es visible en la expresión facial del trabajador y/o la contracción muscular es visible.
ALTO	Actividad pesada, con resistencia.
MEDIO	Actividad con esfuerzo moderado.
BAJO	No hay esfuerzo aparente, ni resistencia, y existe libertad de movimientos
MANIPULACION MANUAL DE CARGAS	
MUY ALTO	Manipulación manual de cargas con un riesgo extremo de lesión musculoesquelética. Deben tomarse medidas correctivas inmediatamente
ALTO	Manipulación manual de cargas con riesgo probable de lesión. Se deben modificar las condiciones de trabajo tan pronto como sea posible.

¡Antes de imprimir este documento… piense en el medio ambiente!
Cualquier copia impresa de este documento, se considera copia No Controlada

MEDIO	Manipulación manual de cargas con riesgo moderado de lesión musculoesquelética sobre las que se precisa una modificación, aunque no inmediata
BAJO	No se manipulan cargas o si se realiza, no se evidencian riesgos de lesiones musculoesqueléticas. No es necesaria ninguna acción
PSICOSOCIALES	
MUY ALTO	Nivel de riesgo con alta posibilidad de asociarse a respuestas muy altas de estrés. Por consiguiente, las dimensiones y dominios que se encuentran bajo esta categoría requieren intervención inmediata en el marco de un sistema de vigilancia epidemiológica
ALTO	Nivel de riesgo que tiene una importante posibilidad de asociación con respuestas de estrés alto y, por tanto, las dimensiones y dominios que se encuentren bajo esta categoría requieren intervención, en el marco de un sistema de vigilancia epidemiológica
MEDIO	Nivel de riesgo en el que se esperaría unas respuestas de estrés moderada, las dimensiones y dominios que se encuentran bajo esta categoría ameritan observación y acciones sistemática de intervención para prevenir efectos perjudiciales en la salud
BAJO	No se espera que los factores psicosociales que obtengan puntuaciones de este nivel estén relacionados con síntomas o respuestas de estrés significativas. Las dimensiones y dominios que se encuentran bajo esta categoría serán objeto de acciones o programas de intervención, con el fin de mantenerlos en los niveles de riesgo más bajos posibles

En el caso de los peligros químicos se debe valorar teniendo en cuenta la siguiente tabla de equivalencia, clasificación y nivel de deficiencia, se tomará el nivel de deficiencia de acuerdo con el nivel de peligrosidad más alto en cualquiera de los ítems de salud, inflamabilidad y reactividad.

Tabla 32 Determinación de Nivel de deficiencia para peligros químicos

DETERMINACIÓN DEL NIVEL DE DEFICIENCIA (ND) – PELIGROS QUÍMICOS				
INFLAMABILIDAD	**REACTIVIDAD**	**SALUD**	**INFLAMABILIDAD**	**REACTIVIDAD**
MUY ALTO (10)	4	Sustancia o mezclas que con una muy corta exposición pueden causar la muerte o daño permanente aún en caso de atención médica inmediata.	Sustancias o mezclas que se vaporizan rápido o completamente a la temperatura a presión atmosférica ambiental, o que se dispersan y se quemen fácilmente en el aire, (como el propano). Tienen un punto de inflamabilidad por debajo de 23°C (73°F)	Fácilmente capaz de detonar o descomponerse explosivamente en condiciones de temperatura y presión normal.
ALTO (6)	3	Sustancias o mezclas que, bajo una corta exposición, pueden causar daños temporales o permanentes, aunque se dé pronta atención médica.	Líquidos y sólidos que pueden encenderse en casi todas las condiciones de temperatura ambiental.	Capaz de detonar o descomponerse explosivamente, pero requiere una fuente de ignición, debe ser Calentado bajo confinamiento antes de la ignición, reacciona explosivamente con agua o detonara si recibe una descarga eléctrica fuerte.
MEDIO (2)	2	Sustancias o mezclas que bajo su exposición intensa o continua pueden causar incapacidad	Sustancias o mezclas que deben calentarse moderadamente o exponerse a temperaturas altas antes de que ocurra la ignición	Experimenta cambio químico violento en Condiciones de temperatura y presión elevadas, reacciona violentamente con agua o

PÚBLICA

DETERMINACIÓN DEL NIVEL DE DEFICIENCIA (ND) – PELIGROS QUÍMICOS				
INFLAMABILIDAD	**REACTIVIDAD**	**SALUD**	**INFLAMABILIDAD**	**REACTIVIDAD**
		temporal o posibles daños permanentes, a menos que de tratamiento médico rápido.		puede formar mezclas explosivas con agua.
BAJO	1	Sustancias o mezclas que bajo su exposición causan irritación, pero sólo daños residuales menores aún en ausencia de tratamiento médico	Sustancias o mezclas que deben precalentarse antes de que ocurra la ignición, cuyo punto de inflamabilidad es superior a 93 °C (200°F)	Normalmente estable, pero puede llegar a ser inestable en condiciones de temperatura y presión elevadas.
	0	Sustancias o mezclas que bajo su exposición en condiciones de incendio no ofrecen otro peligro que el material combustible ordinario	Sustancias o mezclas que no se queman como el agua expuestos a una temperatura de 815.5 °C (1500°F) por más de 5 minutos.	Normalmente estable e incluso bajo exposición al fuego y no reactivo con agua.

Nota: Para dar un valor cuantitativo a los peligros higiénicos, se podría tomar el anexo D valoración cuantitativa de los peligros higiénicos de la GTC 45:2012, en donde se podrá valorar de manera objetiva bien porque hay una legislación que indica unos valores máximos, bien porque existe una normativa nacional o internacional sobre la cual se puede comparar los resultados obtenidos.

Estos valores no determinan una frontera entre salud y enfermedad, cada individuo responde de manera diferente a la dosis de contaminante recibida, entendiendo por dosis la cantidad de contaminante a la que está expuesto el trabajador por el tiempo de exposición; así, a mismas dosis las personas se ven afectadas de manera diferente).

Posterior a esto se determina el nivel de exposición de acuerdo con la tabla 33.

Tabla 33 Parámetros para determinar el valor de la exposición

DETERMINACIÓN DEL NIVEL DE EXPOSICIÓN (NE)		
NIVEL DE EXPOSICIÓN	**VALOR DEL NE**	**SIGNIFICADO**
Continua (EC)	4	La situación de exposición se presenta sin interrupción o varias veces con tiempo prolongado durante la jornada laboral.
Frecuente (EF)	3	La situación de exposición se presenta varias veces durante la jornada laboral por tiempos cortos.
Ocasional (EO)	2	La situación de exposición se presenta alguna vez durante la jornada laboral y por un periodo de tiempo corto.
Esporádica (EE)	1	La situación de exposición se presenta de manera eventual.

PÚBLICA

Para determinar el Nivel de Probabilidad NP, se combinan los resultados del nivel de deficiencia y el nivel de exposición.

Tabla 34 Parámetros para determinar el nivel de probabilidad

DETERMINACIÓN DEL NIVEL DE PROBABILIDAD (NP)					
NIVELES DE PROBABILIDAD NP		NIVEL DE EXPOSICIÓN (NE)			
		4	3	2	1
NIVEL DE DEFICIENCIA (ND)	10	MA - 40	MA - 30	A - 20	A - 10
	6	MA - 24	A - 18	A - 12	M - 6
	2	M - 8	M - 6	B - 4	B - 2

De acuerdo con el resultado obtenido se realiza la clasificación del nivel de probabilidad de acuerdo con la siguiente tabla.

Tabla 35 Determinación del Nivel de Probabilidad

DETERMINACIÓN DEL NIVEL DE PROBABILIDAD (NP)		
NIVEL DE PROBABILIDAD	VALOR DEL NP	SIGNIFICADO
Muy Alto (MA)	Entre 40 y 24	Situación deficiente con exposición continua, o muy deficiente con exposición frecuente. Normalmente la materialización del riesgo ocurre con frecuencia.
Alto (A)	Entre 20 y 10	Situación deficiente con exposición frecuente u ocasional, o bien situación muy deficiente con exposición ocasional o esporádica. La materialización del Riesgo es posible que suceda varias veces en la vida laboral
Medio (M)	Entre 8 y 6	Situación deficiente con exposición esporádica, o bien situación mejorable con exposición continuada o frecuente. Es posible que suceda el daño alguna vez.
Bajo (B)	Entre 4 y 2	Situación mejorable con exposición ocasional o esporádica, o situación sin anomalía destacable con cualquier nivel de exposición. No es esperable que se materialice el riesgo, aunque puede ser concebible.

El nivel de consecuencia se determina de acuerdo con los siguientes parámetros.

Tabla 36 Determinación del nivel de consecuencias

DETERMINACIÓN DEL NIVEL DE CONSECUENCIAS (NC)		
NIVEL DE CONSECUENCIAS	VALOR DEL NC	SIGNIFICADO
		Daños Personales
Mortal o Catastrófico (M)	100	Muerte (s).
Muy grave (MG)	60	Lesiones o enfermedades graves irreparables (Incapacidad permanente parcial o invalidez).
Grave (G)	25	Lesiones o enfermedades con incapacidad laboral temporal (ILT).
Leve (L)	10	Lesiones o enfermedades que no requieren incapacidad.

Nota: Para evaluar el nivel de consecuencias, tenga en cuenta la consecuencia directa más grave que se pueda presentar en la actividad valorada.

Finalmente, el nivel de riesgo se calcula teniendo en cuenta la tabla 36 y se clasifica en 4 niveles como se muestra en la tabla 37.

Tabla 37 Determinación del nivel de riesgo

DETERMINACIÓN DEL NIVEL DE RIESGO (NR)					
Nivel de Riesgo NR = NP X NC		**NIVEL DE PROBABILIDAD (NP)**			
		40-24	**20-10**	**8-6**	**4-2**
NIVEL DE CONSECUENCIAS (NC)	**100**	**(I)** 4000- 2400	**(I)** 2000 – 1200	**(I) 800-600**	**(II) 400 – 200**
	60	**I 2400 -1440**	**(II)** 1200 - 600	**(II) 480 – 360**	**II 240 III 120**
	25	**I 1000 - 600**	**(II) 500 -250**	**II 200-150**	**III 100 – 50**
	10	**(II) 400-240**	**II 200 III 100**	**III 80-60**	**III 40 IV 20**

Tabla 38 Significado del nivel de riesgo

SIGNIFICADO DEL NIVEL DE RIESGO		
NIVEL DE RIESGO Y DE INTERVENCIÓN	**VALOR DE NR**	**SIGNIFICADO**
I	4000 – 600	Situación crítica. Suspender actividades hasta que el riesgo esté bajo control. Intervención urgente.
II	500 – 150	Corregir y adoptar medidas de control de inmediato.
III	120 – 40	Mejorar si es posible. Sería conveniente justificar la intervención y su rentabilidad
IV	20	Mantener las medidas de control existentes, pero se deberían considerar soluciones o mejoras y se deben hacer comprobaciones periódicas para asegurar que el riesgo aún es aceptable.

Para el peligro de tránsito:
Se implementa la metodología establecida en la Resolución 40595 del 2022 del Ministerio de Transporte, esta herramienta valorar los riesgos a través del mapa de calor en términos de probabilidad y exposición.

Nivel de exposición:

Tabla 39 Significado del nivel de exposición

NIVEL DE EXPOSICIÓN	VALOR	DESCRIPCIÓN
Frecuente	3	La exposición riesgo vial se presenta más de 6 horas al día.
Ocasional	2	La exposición riesgo vial se presenta entre 3 y 6 horas al día.
Esporádica	1	La exposición riesgo vial se presenta menos de 3 horas al día.

Luego se define el nivel de probabilidad con respecto a los controles que se tienen implementados para reducir el riesgo vial:

Nivel de probabilidad:

Tabla 40 Significado del nivel de probabilidad

NIVEL DE PROBABILIDAD	VALOR	DESCRIPCIÓN
Muy Probable	3	No se tienen establecidos controles eficaces.
Poco Probable	2	Se tienen controles, pero su eficacia es baja.
No es Probable	1	Se tienen controles eficaces.

Nota: No se tiene en cuenta el nivel de consecuencia debido a que, en seguridad vial siempre va a ser crítico y afectaría la gestión que se puede realizar sobre cada variable.

Valoración del nivel de riesgo:

Tabla 41 Significado del nivel de la valoración de riesgo

NIVEL DE RIESGO			NIVEL DE PROBABILIDAD		
			1	2	3
			No es Probable	Poco Probable	Muy Probable
NIVEL DE EXPOSICIÓN	Frecuente	3	3	6	9
	Ocasional	2	2	4	6
	Esporádica	1	1	2	3

Nivel de Riesgo:

Tabla 42 Significado del nivel de riesgo

NIVEL DE RIESGO	VALOR DE NR
I: Crítico	6-9
II: Moderado	3-4
III: Bajo	1-2

Aceptabilidad del riesgo: Se determina según el nivel de riesgo, de acuerdo con la siguiente tabla:

Tabla 43 De aceptabilidad del riesgo

ACEPTABILIDAD DEL RIESGO		
NIVEL DE RIESGO	SIGNIFICADO EXPLICACIÓN	
I	No aceptable	Situación crítica, corrección urgente
II	No aceptable o Aceptable con control específico	Corregir o adoptar medidas de control
III	Mejorable	Mejorar el control existente
IV	Aceptable	No es necesario intervenir, salvo que un análisis más preciso lo justifique.

Nota: Si el riesgo es No aceptable, se deberá intervenir de forma prioritaria y se seguirá lo establecido en el *"Procedimiento Acciones Correctivas P2.MI"* hasta que el riesgo este bajo control.

PÚBLICA

Nota: Así mismo se deben considerar también los controles administrativos que la entidad ha implementado para disminuir el riesgo.

j. Criterios para establecer controles: Al valorar el riesgo y verificar su aceptabilidad, se deben determinar criterios tales como:

- **No. de expuestos:** Se debe determinar la cantidad de personas expuestas a este peligro para establecer el alcance del control que se va a implementar. Entre los expuestos se deben considerar los colaboradores de **Planta, Contratistas, Pasantes, Visitantes**, e incluir los datos de manera individual en la matriz de identificación de peligros, valoración de riesgos y determinación de los controles.
- **Consecuencia:** Identificar la peor consecuencia del peligro asociado con el fin de determinar el control que mitigue dicha consecuencia. Para ello puede elegir de la lista despegable denominada *"**Consecuencia"*** las opciones de accidente, enfermedad laboral, enfermedad común o muerte.
- Existencia de requisito legal y otros específicos o asociados (si/no): Establecer si existe o no un requisito legal específico asociado para tener parámetros de priorización en la implementación de las medidas de intervención. Debe ser coherente con lo registrado en la Matriz de Verificación de Requisitos Legales según lo indicado en el P4.MI Procedimiento Identificación y Evaluación de Requisitos Legales y Otros Requisitos.

k. **Medidas de Intervención:** Se deben seleccionar las medidas de intervención de acuerdo con las opciones descritas en la lista despegable denominada *"Medidas de Intervención".*

- **Eliminación:** Modificar un diseño para eliminar el peligro, por ejemplo, introducir dispositivos mecánicos de alzamiento para eliminar el peligro de manipulación manual. Eliminación de la fuente del peligro.
- **Sustitución:** Medida que se toma a fin de reemplazar un peligro por otro que no genere riesgo o que genere menos riesgo.
  Nota: Para efectos de seguridad vial se denominará "evitarlo", y se registraran las medidas de intervención en el ítem de "sustitución".
- **Controles de ingeniería:** Instalar sistemas de ventilación, protección para las máquinas, enclavamiento, cerramientos acústicos, etc.
- **Controles administrativos:** Señalización, advertencias, instalación de alarmas, procedimientos de seguridad, inspecciones de los equipos, controles de acceso, capacitación del personal.
  Equipos / elementos de protección personal: Gafas de seguridad, protección auditiva, máscaras faciales, sistemas de detención de caídas, respiradores y guantes.

l. Medición de la Eficacia: Una vez definidos los controles y las acciones realizadas, se deberá evaluar su cumplimiento, así mismo el riesgo residual el cual corresponde al nivel del riesgo resultante una vez de implementados los controles, con el fin de medir su eficacia e identificar la necesidad de modificar o introducir nuevos controles.

- Eficacia positiva: Son aquellos peligros que presentan una reducción en la aceptabilidad del riesgo, debido a la disminución del nivel de deficiencia, exposición o consecuencia de los controles implementados. Es decir que los controles son eficaces.

PUBLICA

- Eficacia Lineal: Son aquellos peligros en los que no hubo cambio de aceptabilidad del riesgo, es decir, que el nivel de riesgo inherente mostró ser eficaces ya que su controló su materialización.
- Eficacia negativa: Aquellos peligros en los que hubo incremento de aceptabilidad del riesgo, debido al aumento del nivel de deficiencia, exposición o consecuencia lo que indicaría la generación de nuevos controles o cambios de los mismos, es decir que los controles no son lo suficientemente eficaces.

m. Flujo de aprobación de matriz de peligros: Una vez creado en el aplicativo el flujo de aprobación de identificación de peligros, valoración de riesgos y determinación de controles, se procede a cargar la matriz generada por quien elabora, posterior se deberá dan continuidad de acuerdo con la siguiente tabla.

Tabla 44 Aprobación Peligros

EJE	NIVEL	ELABORAR	REVISAR	VALIDAR	APROBAR
SG-SST	**Sede de la Dirección General**	Profesional del Grupo de Desarrollo del Talento Humano de la Dirección de Gestión Humana	Coordinador del Grupo de Desarrollo del Talento Humano	Director(a) Gestión Humana	Director(a) Gestión Humana
	Regional y Centros Zonales	Profesional del Grupo Administrativo, Gestión Humana o Gestión de Soporte	Profesional del Grupo de Desarrollo del Talento Humano de la Dirección de Gestión Humana	Director Regional Coordinador administrativo Gestión de soporte o Gestión Humana en la Regional. Coordinador del Centro Zonal	Director(a) Gestión Humana

Nota 1: Los debidos soportes de revisión y aprobación deben ser conservados por quien elabora la matriz de peligros, valoración de riesgos y determinación de controles, e incluirlos en la carpeta indicada por el Equipo de Seguridad y Salud en el Trabajo de Gestión Humana.

Nota 2. Se deberá comunicar la matriz de peligros, valoración de riesgos y determinación de controles a los colaboradores a través de medios electrónicos o mesas de trabajo. Así mismo serán publicadas en el micrositio del eje de SST.

Al aplicar un control determinado se deberían considerar los costos relativos y la gestión de estos, los beneficios de la reducción del nivel de riesgo, y la confiabilidad de las opciones disponibles. Igualmente se debe tener en cuenta que entre las opciones de tratamiento se pueden incluir temas como: inspecciones, ajustes a procedimientos o documentación en general, y demás.

El seguimiento está a cargo del Equipo de Seguridad y Salud en el Trabajo de la Dirección de Gestión Humana, apoyados con los Profesionales del Grupo Administrativo, Gestión Humana o Gestión de Soporte a nivel nacional. Adicionalmente, se debe realizar un monitoreo por parte de los responsables, con el fin de garantizar que los peligros a los que están expuestos los colaboradores

PÚBLICA

se vean reflejados en la matriz respectiva y tengan tratamiento, de lo contrario debe ser informado al equipo de Seguridad y Salud en el Trabajo de la Dirección de Gestión Humana.

Luego de contar con el levantamiento de la información de las matrices a Nivel Nacional, se realizará la consolidación final de peligros en SST del ICBF por parte del equipo de Seguridad y Salud en el Trabajo de Gestión Humana, quienes realizarán una priorización para implementar controles encaminados a su mitigación y mejora continua.

4. GESTIÓN DE RIESGOS Y OPORTUNIDADES SISTEMA DE GESTIÓN DE SEGURIDAD Y SALUD EN EL TRABAJO – SGSST.

La Entidad determina y evalúa los riesgos y oportunidades que son pertinentes para los resultados previstos para el Sistema de Gestión de Seguridad y Salud en el Trabajo, relacionados con los peligros y con los requisitos legales y otros requisitos, con el fin de prevenir o reducir efectos no deseados, y lograr la mejora continua.

El Instituto ha empleado herramientas para la participación y consulta de los colaboradores, entre las cuales se destacan la actualización del contexto interno y externo de la Entidad basado en la metodología DOFA, así como, la actualización de las necesidades y expectativas de cada una de las partes interesadas definidas por la entidad.

Una vez recolectada y analizada la información, la evaluación de los riesgos se realiza por medio de la metodología establecida en la Guía de Riesgos del Departamento Administrativo de la Función Pública (DAFP) y la Norma Técnica ISO 31000, registrando la información en el Formato F1.G3.MI Matriz de Riesgos Ambientales y del Sistema de Gestión Seguridad y Salud en el Trabajo, teniendo en cuenta los siguientes criterios:

- Análisis del Contexto
- Identificación del Riesgo
- Identificación de Causas
- Identificación de Consecuencias
- Análisis del Riesgo
- Controles Existentes
- Plan de Tratamiento para Riesgos

4.1. Políticas Operativas para la Gestión de Riesgos y Oportunidades para el Sistema de Gestión de la Seguridad y Salud en el Trabajo:

1. La revisión y validación de los riesgos para el Sistema de Gestión de Seguridad y Salud en el Trabajo, se realizará mínimo una vez al año desde la Sede de la Dirección General, bajo los siguientes criterios:
   - Expedición y/o modificación de los requisitos legales y otros requisitos.
   - Cambios estratégicos en los procesos que incidan en la Seguridad y Salud en el Trabajo.
   - Resultados de la identificación y cambios en el contexto interno y externo.
   - Resultados de la identificación de peligros, valoración de riesgos y determinación de controles.

PÚBLICA

- Resultados de las necesidades y expectativas de las partes interesadas.
- Resultados y decisiones de la Revisión por la Dirección.
- Política y objetivos del Sistema de Gestión de Seguridad y Salud en el Trabajo.
- Gestión de procesos de cambio.
- Retroalimentación de la participación y consulta.
- preparación y respuesta ante emergencias.

Nota: Cuando se requiera realizar la actualización se debe documentar en el formato respectivo.

2. La gestión de riesgos inicia con la identificación y análisis, definición de controles, las actividades y fechas de cumplimiento de los planes de tratamiento.
3. Con base en los riesgos identificados y los planes de tratamiento aprobados por el Director de Gestión Humana líder del eje, las regionales deben revisar y validar, y en caso de requerirse pueden sugerir nuevas actividades y fechas para el plan de tratamiento.
4. La matriz de riesgos y planes de tratamiento deben ser aprobada por el Director Regional junto con los Coordinadores Administrativos, de Gestión Humana y Gestión Soporte, y Referentes de Seguridad y Salud en el Trabajo, mediante acta de reunión, la cual debe estar firmada por los responsables.
5. Para la Sede de la Dirección General la identificación de riesgos del Sistema de Gestión de SST, la realizan los Profesionales de Seguridad y Salud en el Trabajo y es aprobada por el Director de Gestión Humana como líder del Eje.
6. Las fechas de ejecución de las actividades no podrán superar la fecha del 15 de diciembre de cada vigencia. Así mismo, las acciones de los planes de tratamiento deberán tener relación directa con los riesgos identificados.
7. Una vez las matrices de riesgos para el Sistema de Gestión de Seguridad y Salud en el Trabajo son aprobadas, deberán realizar la divulgación de los riesgos y los planes de tratamiento con las actividades para su mitigación.
8. Se realizará el proceso de socialización de resultados de riesgos de Seguridad y Salud en el Trabajo de manera anual mediante la rendición de cuentas según lo establecido en el Plan de Trabajo.
9. En las Regionales los Referentes SST son los responsables de realizar las acciones del plan de tratamiento, así como los controles establecidos.
10. Los Profesionales de Seguridad y Salud en el Trabajo serán los responsables de la revisión, retroalimentación y seguimiento al cumplimiento de las acciones de los planes de tratamiento formulados por las Regionales y la Sede de la Dirección General.
11. Las modificaciones de planes de tratamiento para los riesgos del Sistema de Gestión de SST durante la vigencia, deberá realizarse vía correo electrónico remitido por el Director Regional al líder de eje, a más tardar diez (10) días calendario antes de la fecha de corte. Lo anterior, con el fin de que el Director de Gestión Humana evalué las modificaciones y tomé las acciones correspondientes para monitoreo de los riesgos.
12. Cuando el resultado de la evaluación de un riesgo este en crítico y se presente durante la vigencia incumplimiento reiterativo de los planes de tratamiento o cuando se presenten materializaciones de los riesgos, el líder del eje evaluará la situación para tomar las acciones correspondientes.
13. Si se evidencia la materialización de un riesgo para el Sistema de Gestión de Seguridad y Salud en el Trabajo, el responsable del proceso debe realizar una acción correctiva en el aplicativo de acciones de mejora de acuerdo con el respetivo procedimiento.
14. Identificar y gestionar las oportunidades de mejora derivadas del análisis de riesgos e

PÚBLICA

implementación de los planes de tratamiento.

4.2. Seguimiento y reporte

El monitoreo y revisión de los riesgos y controles establecidos, se realiza trimestralmente por parte de los Referentes SST y Profesionales SST teniendo en cuenta las fechas de cumplimiento definidas para cada actividad del plan de tratamiento (fecha de inicio- fecha final), registrando los resultados de cada una de las actividades desarrolladas en las Matriz de Riesgos y en el informe de gestión trimestral; así como el cargue de cada uno de los soportes correspondientes a los controles en la carpeta compartida. El reporte de cumplimiento de las acciones de los planes de tratamiento por parte de las Regionales se debe realizar dentro de los primeros cinco (5) días hábiles siguiente a la fecha de corte.

5. GESTIÓN DE RIESGOS DE EMERGENCIA[3]

El ICBF para cumplir con su misión en cada sede de las sedes administrativas, Direcciones Regionales y Centros Zonales y enfrentar de manera oportuna, eficiente y eficaz las situaciones de calamidad, desastre o emergencia según el caso, en sus distintas fases, debe establecer las diversas amenazas y vulnerabilidades que según su origen (natural o antrópico) generan algún tipo de impacto en su operación. De esta manera, es necesario contemplar el riesgo como el daño potencial que puede causar, sobre la población y sus bienes, la infraestructura, el ambiente y la economía pública y privada, pueda causarse por la materialización de amenazas, definiéndolo como el producto entre Probabilidad (P) y Severidad (S) en función de tales condiciones amenazantes y las particularidades de vulnerabilidad.

Sobre esta relación se deben establecer medidas de planificación para el control y reducción de riesgos. En una adecuada evaluación se debe considerar la naturaleza del riesgo, su facilidad de acceso o vía de contacto (posibilidad de exposición), las características del sector y/o población expuesta (receptor), la posibilidad de que ocurra y la magnitud de exposición y sus consecuencias, para de esta manera, definir medidas que permitan minimizar los impactos que se puedan generar. Dentro de este análisis se deben identificar los peligros asociados con cada uno de los riesgos, entendiendo a estos peligros como el potencial de causar algún tipo de daño.

Dichas acciones se deben plasmar en el marco de un Plan de Emergencia y Contingencias a nivel Nacional, Regional y Zonal.

5.1. Objetivo General

Definir procedimientos claros, precisos y únicos que, junto con los planes de acción y contingencia, permitan dar una respuesta oportuna ante cualquier amenaza que ponga en riesgo a los colaboradores y demás personas involucradas que se encuentren en las instalaciones del Instituto Colombiano de Bienestar Familiar-ICBF.

[3] Información basada en el documento: Metodologías de análisis de riesgo. Documento soporte. Guía para elaborar planes de emergencias y contingencias. Fondo de Prevención y Atención de Emergencias – Fopae

PÚBLICA

Objetivos Específicos

- Identificar las amenazas de origen natural, social y antrópicas no intencionales que pueden generar emergencias dentro y fuera de la institución.
- Valorar y evaluar el riesgo frente a las amenazas identificadas mediante la metodología de valoración preliminar del riesgo establecida.
- Analizar la vulnerabilidad frente a las amenazas identificadas que pueden afectar las sedes del Instituto de Bienestar Familiar-ICBF.
- Identificar los recursos físicos, humanos y tecnológicos con que cuenta el ICBF para la prevención, preparación y respuesta ante emergencias. Planificar acciones para prevenir o mitigar los impactos ambientales adversos provocados por situaciones de emergencia.
- Establecer el Puesto de Mando Unificado-PMU para la atención eficiente y eficaz, de la emergencia.
- Diseñar e implementar planes de acción y contingencia para la prevención y atención de emergencias.
- Realizar simulacros como mínimo una (1) vez al año.
- Conformar, capacitar, entrenar y dotar la brigada de emergencias.
- Definir protocolos y acciones orientadas a generar en los brigadistas, colaboradores y visitantes el conocimiento y entrenamiento para actuar de manera oportuna, segura y efectiva frente a condiciones de riesgo y amenazas.

5.2. Condiciones Generales

- De acuerdo con los resultados de la aplicación de la metodología de análisis preliminar del riesgo, la identificación y valoración de amenazas se incluirán los planes de contingencia de las amenazas ubicadas en la matriz de riesgos en las columnas D y E del 1 al 6 en la escala de probabilidad y columna C 3,4,5 y 6 en la escala de probabilidad.
- En las formulaciones y actualizaciones de los PEC se debe contar con la participación de los profesionales de los ejes del SIGE, es importante que se involucren brigadistas, COPASST y grupos de interés.

5.3. Identificación de Amenazas

Teniendo en cuenta la necesidad de conocer la condición latente derivada de la posible ocurrencia de un fenómeno físico de origen natural, socio-natural o antrópico no intencional, que puede causar daño a la población y sus bienes, la infraestructura, el ambiente y la economía pública y privada, es necesario identificar las amenazas, conforme el formato matriz de valoración de riesgos de emergencia. A continuación, se relacionan las posibles amenazas a identificar según la metodología:

Para la identificación de amenazas a continuación se relacionan las siguientes:

Tabla 39 Clasificación de Amenazas

Amenazas Naturales	
Sequías	Inundaciones
Creciente Súbita	Movimientos en masa
Actividad Volcánica	Actividad Sísmica
Tsunami	Vendaval
Huracán	Altas precipitaciones

PÚBLICA

Tormenta Eléctrica	Brotes de enfermedades epidémicas
Enfermedades contagiosas o de origen animal o vegetal	
Amenazas Antrópicas	
Colapso estructural	Fallo en el suministro de redes físicas (energía, gas, agua e internet)
Incendios	Perdida de contención de materiales peligrosos y/o derrames
Falla en sistema de recolección de residuos sólidos	Explosión
Contaminación de alimentos	
Amenazas Sociales	
Atentados	Huelgas y/o asonadas
Hurtos	

5.4. Metodología de Análisis Preliminar de Riesgos

- **Consideraciones técnicas**

La metodología señala los principales aspectos que deben considerarse para efectos de establecer el análisis preliminar de riesgos, integrando de manera articulada elementos de Salud, Ambiente y Riesgo Industrial, para lo cual se dividió en 4 partes cada una con peso dentro de la evaluación total:

1. Matriz de riesgos – 10%, 20%, 30% o 40%
2. Elementos de Gestión en Seguridad, Salud y Ambiente – 20%
3. Aspectos ambientales – 20%
4. Otras características – 20%

Cada componente tiene un porcentaje asignado, de manera tal que un valor alto significa que la Organización representa un riesgo de tal magnitud para el lugar en valoración.

- **Matriz de riesgos**

La metodología de análisis preliminar de riesgos es una iniciativa patrocinada por el Departamento para la Industria y medio ambiente del programa de las Naciones Unidas para el Medio Ambiente (PNUMA), en cooperación con la Asociación de Productos Químicos de estados Unidos y el Consejo Europeo de las Federaciones de la industria química.

El énfasis se realiza en los accidentes industriales que representen una amenaza potencial para las personas, la propiedad y el ambiente, para que a través de este conocimiento en el nivel de toma de decisiones tengan mayores elementos de juicio para establecer y mejorar la preparación para situaciones de emergencia.

El análisis de riesgo busca medir las consecuencias de un accidente contra las probabilidades de que este llegue a ocurrir.

La probabilidad de que suceda un accidente y sus consecuencias raramente puede llegar a calcularse en forma exacta (matemática). Sin embargo, con frecuencia se pueden estimar con la precisión suficiente para poder establecer una base que permita tomar medidas prácticas para contener los riesgos.

PÚBLICA

El término “riesgo” incluye dos aspectos:

1. La probabilidad de que un accidente ocurra dentro de cierto período de tiempo.
2. Las consecuencias para la población, las propiedades y el ambiente.

En el desarrollo del análisis es importante tomar en cuenta lo siguiente:

- El potencial de la amenaza, por ejemplo, la cantidad y el grado de toxicidad de sustancias químicas peligrosas o la energía almacenada, y la clase de accidentes que pueden ocurrir.
- La ubicación de la amenaza, la vulnerabilidad de los elementos amenazados en las inmediaciones, la capacidad de respuesta de la Organización, y los métodos de descontaminación, una vez haya concluido la etapa crítica.
- Las consecuencias para la economía local.
- El peligro de que el elemento amenazado haga que el accidente se agrave.

5.5. Factores que Afectan la Amenaza y el Riesgo

En la evaluación de amenazas y de elementos vulnerables, es necesario considerar algunos factores que pueden acrecentar o disminuir el riesgo. Entre estos se cuentan:

- Condiciones extremas, por ejemplo, cuando se manejan sustancias peligrosas.
- Los efectos del almacenamiento de varias sustancias juntas.
- El hecho de que los envases de las sustancias químicas estén mal etiquetados o no lleven sello alguno.
- La distancia de seguridad que se guarda entre la amenaza y el elemento vulnerable para lograr limitar los efectos por repercusión.
- La capacitación del personal para evitar el daño ocasionado por el evento, y el establecimiento de canales de comunicación efectivos para avisar oportunamente a las brigadas, organismos de socorro y elementos vulnerables.
- Los efectos de fuerzas naturales como lluvia, viento, avalanchas, entre otros.
- El daño posible o probable y el número estimado de afectados.
- La posibilidad de poder detectar una amenaza cuando aún se encuentra en su etapa inicial.
- La probabilidad y los posibles efectos de un acto de sabotaje.

El desarrollo de la metodología presentada implica el desarrollo de 7 pasos:

1. Bases para el análisis
2. Inventario de las fuentes de riesgo
3. Identificación de las amenazas
5. Clasificación de las consecuencias
6. Determinación de la Probabilidad y Asignación de Rangos
7. Presentación de los resultados del análisis

5.6. Valorización de las Consecuencias

Una vez identificadas las amenazas, se procede a determinar el nivel de riesgo, las cuales deben ser ajustadas según el análisis a desarrollar ya que cada condición es particular dentro de la Matriz

PÚBLICA

de valoración de riesgos de emergencia

Tabla 40 Clasificación de consecuencias para la vida y la salud

Clasificación de consecuencias para la vida y la salud	
Clase	**Características**
1. Poco importantes	Padecimientos ligeros durante un día o menos
2. Limitadas	Lesiones menores, malestar que perdura por una semana o menos
3. Graves	Algunas heridas graves, serias complicaciones
4. Muy graves	Muerte de al menos una persona, y/o varios heridos (10) de gravedad y/o hasta 50 evacuados
5. Catastróficas	Varias muertes, mayor igual a 11 heridos graves y/o más de 50 evacuados

Tabla 47 Clasificación de consecuencias para el ambiente

Clasificación de consecuencias para el ambiente	
Clase	**Características**
1. Poco importantes	No hay contaminación
2. Limitadas	Hay baja contaminación y sus efectos están contendidos
3. Graves	Hay baja o media contaminación y sus efectos están muy difundidos
4. Muy graves	Hay alta contaminación y sus efectos están contenidos
5. Catastróficas	Hay muy alta contaminación y sus efectos están muy difundidos

Tabla 41 Clasificación según la velocidad de desarrollo

Clasificación según la velocidad de desarrollo	
Clase	**Características**
1. Advertencia precisa y anticipada	Efectos contenidos/ningún daño
2. Media	Alguna propagación/pocos daños
3. Alta	Daños considerables/efectos contenidos
4. Sin advertencia	Desconocidos hasta que los efectos se han desarrollado completamente. Efectos inmediatos (explosión)

Tabla 42 Escala de Probabilidad

Escala de Probabilidad	
Clase	**Características**
1.Improbable	Una vez cada 20 a 50 años
2.Poco probable	Una vez cada 10 a 20 años
3.Probable	Una vez cada 5 a 10 años
4. Medianamente probable	Una vez de 1 a 5 años
5.Bastante Probable	Una vez por año
6.Muy Probable	Varias veces por año

5.7. Elementos de Gestión en Seguridad y Salud

Se identifican 25 puntos con el fin de disminuir el riesgo teniendo en cuenta que el resultado se clasificara de la siguiente manera:

- De 20 a 25 puntos = 20%
- De 13 a 19 puntos = 15%
- De 7 a 12 puntos = 10%
- De 1 a 6 puntos = 5%

PÚBLICA

- 0 puntos = 0%

Tabla 50 Elementos de Gestión en Seguridad y Salud

SEGURIDAD SI (0)	SI (0)	PARCIALMENTE (0.5)	NO (1)
1-Cuenta con un Sistema de Gestión de Seguridad y Salud en el Trabajo implementado sobre un 95% de los estándares mínimos del SG-SST			
2-La Política de Seguridad, Salud en el Trabajo se encuentra documentada y divulgada entre colaboradores y partes interesadas.			
3-Tiene identificados y evaluados los requisitos legales aplicables para Seguridad y Salud en el trabajo.			
4-Se aplica el procedimiento de evaluación de la implementación del Sistema de Gestión de Seguridad y Salud en el Trabajo.			
5-Cuenta con canales que permitan recolectar inquietudes, oportunidades de mejora, felicitaciones y aportes de los colaboradores en materia de seguridad y salud en el trabajo.			
6-Cuenta con la cartilla de prevención de desastres			
7-Aplica la metodología para la identificación y valoración de los peligros en la sede.			
8- Cuenta con planos detallados de la construcción, instalaciones eléctricas, aguas lluvias, aguas residuales.			
9 -Cuenta con un procedimiento para el reporte e investigación de incidentes de trabajo.			
10 -Cuenta con un plan de emergencias y contingencias para responder a situaciones tales como la alteración de las condiciones normales de operación por amenazas de origen naturales, social y antrópicas no intencionales.			
11-Tiene conformadas y en funcionamiento las brigadas de emergencia.			
12 - Existen recursos y suministros para el personal de las Brigadas			
13 -Tiene actividades de capacitación y entrenamiento para las brigadas de emergencia.			
14 -Tiene establecidos los requisitos necesarios para desempeñar cada trabajo y proporciona a los colaboradores el entrenamiento correspondiente.			
15 -Aplica el procedimiento de inducción, reinducción en Seguridad y Salud en el Trabajo, en el caso de nuevos colaboradores y de refuerzo para colaboradores antiguos.			
16–A los contratistas se les exige el cumplimiento de las normas de seguridad y salud en el trabajo.			
17 -Todos los productos químicos se encuentran identificados conforme a las normas nacionales o internacionales, en lo relacionado con sus riesgos y poseen la correspondiente hoja de seguridad.			
18-Cuenta con equipos redundantes de protección y/o otras medidas de seguridad, donde sea aplicable.			
19- Cuenta con sistemas de prevención (alarmas, extintores, botiquines, detectores de humo, etc.).			
20- Cuenta con esquemas de rutas de evacuación actualizados.			
21- Realiza simulacros al menos una vez al año con participación de todos los colaboradores.			
22. Cuenta con sistemas alternos (planta de emergencia eléctrica, tanques de reserva de agua, bombas eléctricas, etc.)			
23. Cuenta con Sistemas de Recuperación (Pólizas, seguros)			
24. Los colaboradores se involucran en la elaboración de procedimientos tendientes a lograr un ambiente laboral sano y seguro.			

PUBLICA

SEGURIDAD SI (0)	SI (0)	PARCIALMENTE (0.5)	NO (1)
25. Tiene identificados los riesgos y/o peligros por tareas y son conocidos por los colaboradores			

5.8. Aspectos Ambientales

En total se consideran 17 aspectos ambientales y teniendo en cuenta el numeral anterior un puntaje alto significa un riesgo ambiental alto de acuerdo con los siguientes porcentajes

- De 13 a 17 puntos = 20%
- De 9 a 12 puntos = 15%
- De 5 a 8 puntos = 10%
- De 1 a 4 puntos = 5%
- 0 puntos = 0%

Tabla 51 Aspectos Ambientales

AMBIENTE	ENUNCIADO VERDADERO (0)	ENUNCIADO FALSO (1)
1- La Política Ambiental se encuentra escrita y divulgada entre colaboradores, proveedores y otras partes interesadas.		
2- Cuenta con un Plan de Gestión Ambiental de la sede.		
3- Identifica los requisitos legales aplicables en cada sede administrativa.		
4 – En la sede no se generan emisiones.		
5 - La sede cuenta con sistemas de tratamiento de las emisiones.		
6 - La sede no genera vertimientos no domésticos.		
7 - La sede se encuentra conectada a la red de alcantarillado público.		
8 - Los residuos sólidos esperados no contienen características peligrosas.		
9 - La sede realiza simulacros ambientales al menos una vez al año en articulación con el Sistema Integrado de Gestión.		
10 - La sede realiza reducción en la fuente, reciclaje o reutilización.		
11- La sede realiza periódicamente mediciones de residuos.		
12- La sede evalúa los riesgos causados por residuos.		
13 - La sede cuenta con servicios de transporte y disposición final para los residuos.		
14 - La sede cuenta estrategias para la reducción de residuos.		
15 - La sede no cuenta con máquinas y/o equipos generadores de ruido ambiental.		
16 - La sede cuenta con aislamiento que permita la reducción del ruido, tales que garanticen el cumplimiento de la normatividad vigente.		
17 - La sede ha identificado emergencias ambientales dentro de la matriz de valoración de aspectos e impactos ambientales.		
TOTAL		

5.9. Otros Aspectos

Estas características hacen referencia a la ubicación y la vulnerabilidad de los elementos potencialmente amenazados. Se identifica el uso del suelo, si tiene una zona de amortiguamiento que permita atenuar los efectos posibles en caso de emergencia y si cumple con las normas de sismo resistencia del país.

PÚBLICA

Tabla 52 Ubicación y la vulnerabilidad de los elementos

ÁREAS INSTALACIÓN		
ÁREA	**DESCRIPCIÓN**	**m^2**
ÁREA TOTAL INSTALACIÓN		
ÁREA AMORTIGUAMIENTO		
ÁREA	**DESCRIPCIÓN**	**m^2**
ÁREA TOTAL AMORTIGUAMIENTO		
1. RELACIÓN DE ÁREA DE AMORTIGUAMIENTO / ÁREA DE INSTALACIÓN		
2. USO DEL SUELO		
USO RESIDENCIAL O RECREACIONAL (7%)		
USO MIXTO (3,5%)		
USO INDUSTRIAL O COMERCIAL (0%)		
TOTAL, USO DEL SUELO		
3. CUMPLIMIENTO NORMA NSR – 10		
SI CUMPLE (0%)		
NO CUMPLE (7%)		
TOTAL, NORMA NSR - 10		

Teniendo en cuenta que según sea la relación áreas de amortiguamientos/área de la sede, los porcentajes serán:

- Mayor al 75% asignar 0%
- Entre el 50 y el 75% asignar 1.5%
- Entre el 25 y el 49% asignar 3%
- Entre el 10 y el 24% asignar 4.5%
- Menor al 9% asignar 6%

5.10. Matriz de Riesgos

Tabla 43 Matriz de Riesgos

		A	B	C	D	E	
PROBABILIDAD	**Muy Probable**						**6**
	Bastante Probable						**5**
	Medianamente Probable						**4**
	Probable						**3**
	Poco Probable						**2**
	Improbable						**1**
Calificación Matriz Riesgos		**Poco Importante**	**Limitada**	**Graves**	**Muy Graves**	**Catastróficas**	
	40%	**PONDERACIÓN DE LAS CONSECUENCIAS**					

PÚBLICA

Una vez evaluadas cada una de las amenazas en vida, ambiente, propiedad, velocidad de desarrollo y probabilidad, se le asigna a la matriz los siguientes porcentajes:

- 40% RIESGO ALTO Mayor al 80% de las amenazas clasificadas en las columnas D y E de la matriz
- 40% RIESGO ALTO Clasificaciones D y E en la matriz: Igual o mayor al 80% de las amenazas
- 20% RIESGO MEDIO Clasificaciones C, 5 y 6 B: Igual o mayor al 80% de las amenazas
- 10% RIESGO BAJO Clasificaciones 1, 2, 3 y 4 B y 3, 4, 5, y 6 A: Igual o mayor al 80%
- 0% RIESGO MUY BAJO Clasificación 1 y 2 A: Igual o mayor al 80% de las amenazas

5.11. Formato de Evaluación

Una vez realizado los anteriores ítems, se procede a realizar la sumatoria de todos los porcentajes de la siguiente manera:

Tabla 44 Sumatoria de todos los porcentajes

1. RESULTADOS OBTENIDOS	
ASPECTO	**PUNTAJE OBTENIDO**
CLASIFICACIÓN EN LA MATRIZ DE RIESGOS	
PUNTAJE OBTENIDO EN ELEMENTOS DE GESTIÓN EN SEGURIDAD Y SALUD EN EL TRABAJO	
PUNTAJE OBTENIDO EN ELEMENTOS AMBIENTALES	
RELACIÓN ÁREAS DE AMORTIGUAMIENTO/ÁREA ESTABLECIMIENTO	
USO DEL SUELO SITIO DE UBICACIÓN	
CUMPLIMIENTO DE LA NORMA NSR – 10	

2. TABLA REFERENCIA			
ASPECTO	**RANGO**		**ALCANZADO POR LA SEDE**
MATRIZ DE RIESGOS	CLASIFICACIONES D Y E	40,0%	
	CLASIFICACIÓN C, 4B Y 5B	20,0%	
	CLASIFICACIONES 1B, 2B, 3B, 4A, Y 5A	10,0%	
	CLASIFICACIONES 1A, 2A	0,0%	
ELEMENTOS DE GESTIÓN EN SEGURIDAD Y SALUD EN EL TRABAJO	20 - 25 PUNTOS	20,0%	
	13 a 19 PUNTOS	15,0%	
	7 a 13 PUNTOS	10,0%	
	1 a 6 PUNTOS	5,0%	
	0 PUNTOS	0,0%	
ELEMENTOS AMBIENTALES	13 a 17 PUNTOS	20,0%	
	9 a 12 PUNTOS	15,0%	
	5 a 8 PUNTOS	10,0%	
	1 a 4 PUNTOS	5,0%	
	0 PUNTOS	0,0%	
RELACIÓN ÁREAS DE AMORTIGUAMIENTO/ÁREA ESTABLECIMIENTO	MAYOR A 75 %	0,0%	
	ENTRE 50% Y 75 %	1,5%	
	ENTRE 25 % Y 49 %	3,0%	
	ENTRE 10 % Y 24 %	4,5%	
	MENOR AL 9 %	6,0%	

PUBLICA

USO DEL SUELO DEL SITIO DE UBICACIÓN	USO COMERCIALES O INDUSTRIAL	0,0%	
	USO MIXTO (COMERCIAL Y RESIDENCIAL)	3,5%	
	USO RESIDENCIAL O RECREACIONAL	7,0%	
CUMPLIMIENTO DE LA NORMA NSR 10	CUMPLE	0,0%	
	NO CUMPLE	7,0%	
3. SUMATORIA DE PORCENTAJES			
4. INTERPRETACIÓN			

La interpretación de la sumatoria estará sujeta a:

- Mayor a 65% → RIESGO ALTO
- Entre el 30% y el 65% → RIESGO MEDIO
- Menor al 30% → RIESGO BAJO

5.12. Otras Metodologías

A continuación, se mencionan otras metodologías que pueden ser utilizadas para el análisis de riesgo cuya aplicabilidad depende de la disponibilidad de información y del nivel de detalle deseado

- Método Semicuantitativo – GHA
- Técnica Delphi
- Análisis de Árbol De Fallos
- Análisis de Modo y Efecto De Los Fallos - FMEA Y FMECA
- Análisis de Causas Efecto
- Análisis Funcional de Operabilidad - HAZOP
- Análisis de Causa - Raíz
- Análisis de Árbol De Sucesos - ETA
- Análisis de Peligros Y Puntos Críticos De Control – HACCP

6. GESTION DE RIESGOS AMBIENTALES

Introducción

La gestión del riesgo del eje ambiental dentro del Instituto Colombiano de Bienestar Familiar busca asegurar que el Sistema de Gestión Ambiental pueda lograr el cumplimiento de sus objetivos y metas, prevenir y reducir los efectos no deseados, incluyendo las condiciones adversas no deseadas.

De esta forma, la Entidad parte de la consideración de los riesgos teniendo en cuenta el contexto interno y externo de las Regionales y la Sede de la Dirección General; así como, los resultados de la identificación y evaluación de los aspectos e impactos, requisitos legalesy otros requisitos, así mismo, la identificación, evaluación y gestión de los riesgos ambientales.

PÚBLICA

Estos contextos, así como los cambios y desafíos que permanentemente debe enfrentar la Entidad, generan incertidumbre para el logro de los objetivos y el desempeño ambiental. Por lo anterior, se ha establecido una metodología y formato F1.G3.MI MATRIZ DE RIESGOS AMBIENTAL, con el fin de prevenir la probabilidad de ocurrencia y el impacto de estos, a través de la formulación e implementación de controles efectivos.

6.1. Objetivos

Realizar la identificación, análisis y monitoreo de los riesgos que pueden incidir en el desempeño del sistema de gestión ambiental de la Entidad; así como, los controles para su respectiva gestión.

Priorizar y comunicar los riesgos ambientales que deben ser considerados en los procesos de planeación estratégica y toma de decisiones de la Entidad.

6.2. Políticas Operativas para la Gestión de Riesgos del Eje Ambiental

1. La gestión de riesgos del eje ambiental está enfocada al cumplimiento de los objetivos del sistema, por lo cual es considerada estratégica dentro de la organización.

2. La identificación y actualización de los riesgos del eje ambiental se efectuará anualmente desde el nivel central y regional, bajo los siguientes criterios:

    - Expedición y/o modificación a los requisitos legales y otros requisitos de eje ambiental.
    - Cambios en las actividades de los procesos que incidan en el sistema ambiental.
    - Resultados de la identificación del contexto interno y externo del eje ambiental.
    - Resultados de la identificación de aspectos e impactos ambientales.
    - Resultados de la identificación de las necesidades y expectativas de las partes interesadas aplicables al eje ambiental.
    - Resultados de los indicadores del eje ambiental.
    - Resultados y decisiones de la Revisión por la Dirección.
    - Resultados del seguimiento / monitoreo realizado a los riesgos (Materialización de riesgos) relacionados al eje ambiental.

3. La gestión de riesgos inicia con la identificación de los riesgos del eje, análisis de estos, definición de controles para su mitigación y las actividades y fechas de cumplimiento de los planes de tratamiento, los cuales son realizados por los profesionales ambientales de la Sede de la Dirección General y aprobados por el Director Administrativo como líder del Eje, mediante acta de reunión. El acta debe contener las actividades y fechas de los planes de tratamiento asociados a los riesgos.

4. Con base en los riesgos identificados y los planes de tratamiento aprobados por el líder del eje, las regionales validan y aprueban, las actividades propuestas por la Sede de la Dirección General, por parte de los Coordinadores Administrativos / Gestión de Soporte y los referentes ambientales.

PÚBLICA

5. Para la formulación de los planes de tratamiento se deberá definir una acción como mínimo por cada etapa del ciclo PHVA, así mismo, las fechas de ejecución de las actividades del planear no podrán superar el primer cuatrimestre y las fechas del hacer, verificar y actuar no podrán superar la fecha del 15 de diciembre de cada vigencia. Así mismo, las acciones de los planes de tratamiento deberán tener relación directa con los riesgos identificados.

6. Para la formulación de los planes de tratamiento se deberá tener en cuenta los recursos de talento humano, financieros, ajustes de procesos y tecnología y demás que se requieran para la gestión de los riesgos identificados.

7. La aprobación de las matrices de riesgos del eje con sus planes de tratamiento para el nivel regional se realiza mediante acta firmada por los Directores Regionales, Coordinadores Administrativos / Gestión de Soporte y Referentes Ambientales. El acta debe contener las actividades y fechas de los planes de tratamiento asociados a los riesgos.

8. Las actas de aprobación de los riesgos se deben copiar en el repositorio y comunicar a la Dirección Administrativa para que los enlaces correspondientes realicen su respectiva validación final.

9. Una vez las matrices de riesgos ambientales por el nivel central son aprobadas, los referentes y profesionales ambientales deberán realizar la socialización de los riesgos y los planes de tratamiento con las actividades para su mitigación.

10. En las Regionales los referentes ambientales son los responsables de realizar las acciones del plan de tratamiento y reportar los resultados a su enlace en el nivel central, de acuerdo con las fechas establecidas.

11. Los profesionales ambientales de la Dirección Administrativa serán los responsables de la revisión, retroalimentación y seguimiento al cumplimiento de las acciones de los planes de tratamiento formulados por las Regionales y la Sede de la Dirección General.

12. El profesional y/o referente ambiental, será el responsable de los controles establecidos y este deberá garantizar la documentación y evidencias que soporten la implementación.

13. Las modificaciones de planes de tratamiento para los riesgos ambientales durante la vigencia deberán comunicarse vía correo electrónico remitido por el Coordinador Administrativo / Gestión de Soporte al profesional ambiental enlace, a más tardar treinta (30) días calendario antes de la fecha de corte. Lo anterior, con el fin de evaluar las modificaciones y tomar las acciones correspondientes para el monitoreo de los riesgos, posteriormente los ajustes aprobados serán comunicados al Coordinador Administrativo / Gestión de Soporte y referente ambiental, y se verá reflejado en la medición de la gestión de los planes de tratamiento.

14. Cuando se presente durante la vigencia incumplimiento reiterativo de los planes de tratamiento o cuando se presenten materializaciones de los riesgos, se evaluará la pertinencia de generar una acción correctiva teniendo en cuenta, si ésta implica ejecución de recursos y decisiones de la Sede de la Dirección General, igualmente se informará a la Subdirección de Mejoramiento

PÚBLICA

Organizacional, quien revisará la pertinencia de presentar el caso ante el Comité Institucional de Coordinación de Control Interno para su análisis.

15. El referente/profesional ambiental deberá reportar de manera trimestral el cumplimiento de los controles establecidos en la matriz de riesgos al enlace del nivel central, así mismo, deberá cargar en el repositorio del Eje Ambiental las evidencias de cumplimiento de estos.

16. Para la elaboración, revisión y aprobación de las matrices de riesgos del eje ambiental, se deben tener en cuenta los siguientes responsables:

Tabla 45 Aprobación de las matrices de riesgos

RESPONSABLE	NIVEL NACIONAL	NIVEL REGIONAL
ELABORA	Profesionales ambientales de la Dirección Administrativa	
REVISA	Líder del Eje Ambiental (Director Administrativo) Subdirección de Mejoramiento Organizacional	Coordinadores administrativos / Gestión de Soporte y referentes ambientales
APRUEBA	Líder del Eje Ambiental (Director Administrativo)	Director Regional

17. Una vez los riesgos son aprobados desde la Dirección Administrativa, cada responsable en el nivel Nacional y Regional gestionará los riesgos, de acuerdo con los recursos asignados y disponibles.

18. Los riesgos que se materialicen deben continuar identificados en la Matriz de Riesgos.

19. La medición del desempeño, en cuanto a la gestión del riesgo, se hace a partir de los resultados del indicador definido, de acuerdo con el reporte de los riesgos en las Regionales y Sede de la Dirección General.

20. De acuerdo con la clasificación de riesgos, se identifica un riesgo de corrupción, este se deberá gestionar de acuerdo con lo establecido en el numeral 2.1.9 de esta guía.

6.3. Identificación del Riesgo

En esta etapa para la gestión de riesgos de ambientales, se tiene como objetivo identificar los riesgos significativos que deben ser gestionados teniendo en cuenta que el impacto negativo puede afectar el cumplimiento de los objetivos ambientales considerando el contexto externo e interno previamente identificado, las necesidades y expectativas de las partes interesadas, los aspectos e impactos ambientales, requisitos legales y otros requisitos, igualmente, se deberá tener en cuenta los riesgos identificados en la vigencia anterior.

Para el desarrollo de esta etapa se debe tener en cuenta las siguientes fases:

- Análisis de Insumos
- Identificación de Áreas de Impacto
- Identificación de Puntos de Riesgos

PUBLICA

- Identificación de Factores de Riesgo
- Descripción del Riesgo
- Clasificación de Riesgos
- Determinar el Nivel de Aplicabilidad del Riesgo

Las cuales se desarrollarán de la siguiente manera:

6.3.1 Análisis de Insumos

Para iniciar con la identificación de los riesgos ambientales es necesario analizar los siguientes insumos:

- Misión de la entidad.
- Objetivos estratégicos.
- Objetivos del eje ambiental.
- Análisis de contexto interno y externo.
- Necesidades y expectativas de las partes interesadas.
- Resultados de la gestión de riesgos de la vigencia anterior.
- Informes entes de control.
- Informe denuncias presuntos actos de corrupción.
- Resultados validación de riesgos con regionales y centros zonales.
- Recomendaciones informes Oficina de Control Interno

6.3.2 Identificación de Áreas de Impacto

Son las consecuencias a las cuales puede estar expuesta la organización en caso de materializarse un riesgo. Las áreas de impacto pueden ser:

- **Afectación Económica**: Pago de multas o sanciones por incumplimiento de la norma ambiental.
- **Reputacional:** afectación de la imagen y/o credibilidad Institucional.
- **Cumplimiento Objetivos del SGA**: afectación en el cumplimiento de los objetivos establecidos en el sistema de gestión ambiental de la Entidad.

6.3.3 Identificación de puntos de riesgos

En el marco del sistema de gestión ambiental se debe identificar aquellas actividades críticas que pueden provocar la materialización de un riesgo y deben ser controladas. A partir de los puntos de riesgo se realizará en la etapa de valoración la determinación de la probabilidad de ocurrencia.

Tabla 46. Ejemplo de puntos de riesgo y consecuencias de no controlarlos

PUNTO DE RIESGO	POSIBLES CONSECUENCIAS
Identificación y seguimiento de los requisitos ambientales aplicables al ICBF	Sanciones, multas o cierre de las infraestructuras para la prestación del servicio.

PÚBLICA

Sensibilizar y capacitar a los colabores del ICBF y desarrollar evaluaciones de eficacia al capacitado	Incumplimiento de la política ambiental

6.3.4 Identificación de puntos de riesgos

Los factores de riesgo son aquellas fuentes a partir de las cuales se pueden generar los riesgos, en particular para la gestión del ICBF se tendrán en cuenta tres factores, procesos, tecnología e infraestructura.

Tabla 47.Factores de Riesgos ambientales

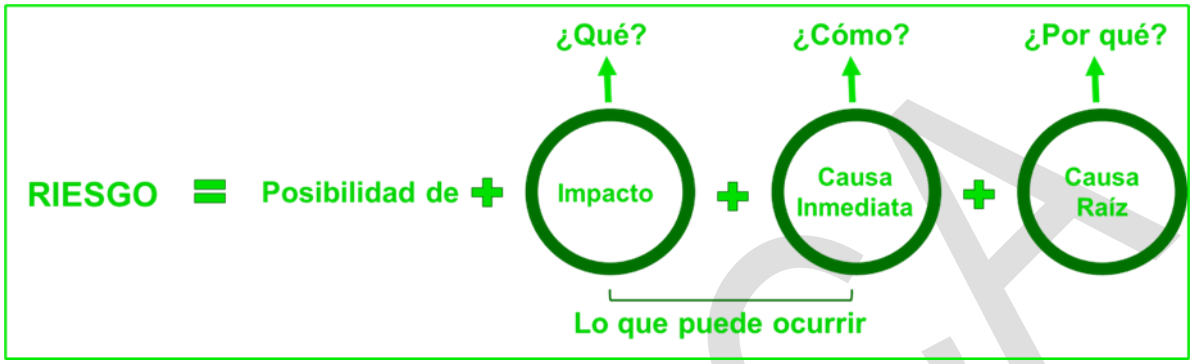
Factor	Definición		Descripción
Procesos	Eventos relacionados con errores en las actividades que deben realizar los servidores de la organización.		Falta de procedimientos
			Falta de capacitación, temas relacionados con el personal
Talento Humano	Son eventos relacionados con posible dolo o intención relacionados con sabotajes, errores, omisión de actividades.		Posibles comportamientos no éticos de los empleados
Tecnología	Eventos relacionados con la infraestructura tecnológica de la entidad.		Caída de redes
			Errores en programas
			Daño en equipos
Infraestructura	Eventos relacionados con la infraestructura física de la entidad		Derrumbes
			Incendios
			Inundaciones
			Daños a activos fijos

6.3.5 Descripción del Riesgo

La descripción del riesgo debe contener información detallada que le permita a cualquier colaborador de la entidad entender fácilmente como se puede manifestar el riesgo, así como sus causas.

De acuerdo con la metodología propuesta por el Departamento Administrativo de la Función Pública –DAFP, se propone la siguiente estructura para la redacción de riesgos:

Imagen 19. Estructura propuesta para la redacción de riesgos



De acuerdo con la estructura se define lo siguiente:

- **Impacto:** Consecuencias a partir de la materialización del riesgo para la entidad.
- **Causa Inmediata:** Circunstancias o situaciones más evidentes sobre las cuales se presenta el riesgo, las mismas no constituyen la causa principal o base para que se presente el riesgo.
- **Causa Raíz:** Causa principal o básica, corresponde a la razón por la cual se puede presentar el riesgo, es la base para la definición de controles en la etapa de valoración del riesgo. Se debe tener en cuenta que para un mismo riesgo pueden existir varias causas que pueden ser analizadas.

6.3.6 Clasificación de Riesgos

Permite agrupar los riesgos identificados en categorías, lo que posibilita a los encargados de la gestión entender mejor la naturaleza del riesgo al que está expuesta la entidad.

Tabla 48. Clasificación de riesgos

Categoría	Descripción
Cumplimiento	Son aquellos riesgos que surgen a partir de errores en la ejecución de los procesos y generan impacto sobre el cumplimiento de los objetivos.
Reputacional	Corresponde a riesgos cuya materialización afectaría la imagen, el buen nombre o la reputación de la entidad ante sus partes interesadas
Económico	Pago de multas por incumplimiento de la norma ambiental.

PÚBLICA

6.3.7 Determinar el Nivel de Aplicabilidad del Riesgo

Una vez identificado el riesgo se debe establecer el o los niveles de la entidad a los que aplica, para esto es importante analizar donde se puede presentar un evento de riesgo materializado. A su vez la definición de aplicabilidad de los riesgos indicará los niveles en los cuales deben ser gestionados o tratados.

Los niveles definidos para la gestión de riesgos en el ICBF son:

- **Nivel Centro Zonal:** se refiere a la gestión en los Centros Zonales.
- **Nivel Regional:** hace referencia a las Direcciones Regionales y sus grupos de trabajo.
- **Nivel Nacional:** se refiere a las dependencias que de acuerdo con la estructura orgánica de la entidad hacen parte de la Sede de la Dirección General.

6.4 Valoración del Riesgo

Consiste en establecer la probabilidad de ocurrencia del riesgo, así como la magnitud o nivel de impacto en la entidad de llegarse a materializar este, con el fin de determinar la zona de riesgo inicial o Riesgo inherente, para posteriormente determinar la zona de riesgo final o Riesgo Residual, el cual se establece una vez se analiza el riesgo inherente frente a los controles implementados para evitar su materialización y mitigar su impacto.

Etapas de la Valoración de Riesgos:

Análisis de Riesgo: En esta etapa se busca establecer la probabilidad de ocurrencia de un riesgo, así como su impacto de llegar a materializarse, con lo cual se determina la zona de riesgo inicial o riesgo inherente.

Evaluación de Riesgo: Consiste en establecer la zona de riesgo final o riesgo residual, la cual se obtiene una vez evaluado el riesgo inherente frente a los controles implementados para prevenir que el riesgo se materialice, así como para moderar el impacto de dicha materialización.

6.4.1 Análisis de Riesgo

Determinar la Probabilidad

La probabilidad de ocurrencia de un riesgo se entiende como la posibilidad de que se produzca una situación que afecte de forma negativa la consecución de los objetivos del sistema de gestión ambiental de la entidad. **De este modo la probabilidad inicial de un riesgo será determinada por el número de veces que se pasa por el punto de riesgo en un periodo de un año, o en otras palabras en número de veces que se realiza una actividad critica durante un año.**

Bajo esta lógica de calificación se elimina la subjetividad del análisis, ya que el resultado de este **depende de la frecuencia con la cual se realiza una actividad**, al mismo tiempo permite determinar un nivel de probabilidad más real para aquellos riesgos que nunca se han materializado.

PÚBLICA

Teniendo en cuenta lo anterior, a continuación, se establecen los criterios para definir la probabilidad de un riesgo ambiental con base en un periodo de 1 año.

Tabla 49. Criterios de probabilidad riesgos ambientales.

Probabilidad de ocurrencia	Frecuencia de la actividad	Probabilidad
Muy baja	La actividad que con lleva el riesgo se ejecuta como máximos 48 veces por año	**20%**
Baja	La actividad que conlleva el riesgo se ejecuta de 49 a 95 veces por año	**40%**
Media	La actividad que conlleva el riesgo se ejecuta de 96 a 143 veces por año	**60%**
Alta	La actividad que conlleva el riesgo se ejecuta mínimo 144 veces al año y máximo 190 veces por año	**80%**
Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 191 veces por año	**100%**

Fuente: Adaptado de la Guía para la administración del riesgo y diseño de controles en entidades públicas del DAFP – V5 y V6.

Determinar el Impacto

Para determinar el nivel de impacto de un riesgo se tendrán en cuenta las 3 áreas de impacto definidas durante la etapa de identificación de riesgos, a saber, afectación económica, reputacional y cumplimiento de los objetivos del Sistema de gestión Ambiental, las cuales deberán ser valoradas teniendo en cuenta la escala determinada.

Es importante señalar que cuando se presenten varios impactos para un riesgo con diferentes niveles en su calificación, se tendrá en cuenta para determinar el nivel de riesgo inherente aquel que tenga la calificación más alta, por ejemplo: *para un riesgo identificado que cuenta con un impacto reputacional menor, un impacto por afectación económica moderado y un impacto al cumplimiento de objetivos del sistema de gestión ambiental mayor; se tomara el más alto, que en este caso correspondería con el cumplimiento de objetivos mayor.*

En consideración de lo anteriormente descrito, se define la escala para la valoración del impacto

Tabla 50. Criterios de impacto riesgos ambientales

Nivel de Impacto	Afectación Económica	Afectación Reputacional	Afectación en el Cumplimiento de los objetivos SGA
Leve 20%	Afectación menor a 10 SMLMV	El riesgo afecta la imagen de algún área de la organización.	Sería imperceptible el impacto en el logro del objetivo SGA.
Menor 40%	Entre 11 y 50 SMLMV	El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, de junta directiva y/o de proveedores.	Impactaría de manera mínima en el logro de los objetivos SGA.
Moderado 60%	Entre 51 y 100 SMLMV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos.	Impactaría moderadamente el logro de los objetivo SGA.
Mayor 80%	Entre 100 y 500 SMLMV	El riesgo afecta la imagen de la entidad con efecto publicitario	Impactaría en alto grado los objetivos SGA.

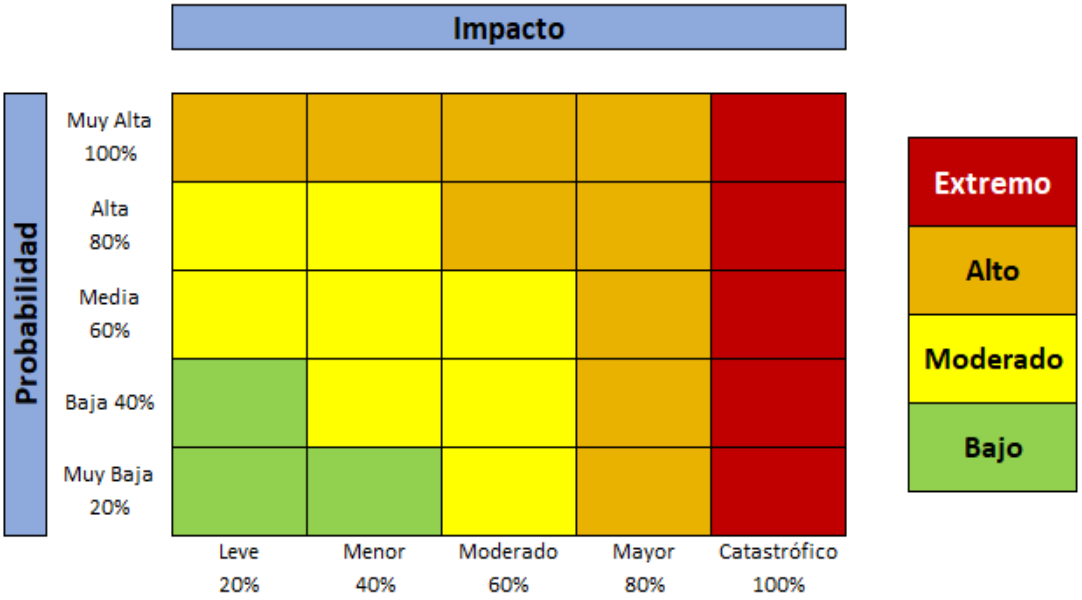
		sostenido a nivel de sector administrativo, nivel departamental o municipal.	
Catastrófico 100%	Mayor a 500 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país.	No se lograría el cumplimiento de los objetivos SGA.

Fuente: Adaptado de la Guía para la administración del riesgo y diseño de controles en entidades públicas del DAFP – V5 y V6.

Nivel Riesgo Inherente

Se puede entender como la valoración del riesgo una vez establecida la probabilidad de ocurrencia, así como su nivel de impacto. Se puede determinar como la relación producto de la combinación de ambas variables, con lo cual se obtiene su ubicación en la matriz de calor, la cual determinará la zona de nivel de riesgo, que a su vez se asocia con severidad de este.

Tabla 51. Matriz de calor



Fuente: Adaptado de la Guía para la administración del riesgo y diseño de controles en entidades públicas del DAFP – V5 y V6.

6.4.2 Evaluación de Riesgos

Identificación de Controles

Para describir un control se debe tener propone la siguiente estructura en su redacción:

a. **Responsable de ejecutar el control:** Debe establecerse el cargo o rol de quien ejecuta el control o garantiza su ejecución.
b. **Acción:** Debe indicar el cómo se realiza la ejecución del control
c. **Periodicidad:** Debe indicarse la frecuencia en determinado tiempo en la cual se ejecuta el control (semestral, trimestral, mensual, semanal, diaria, varia veces al día, cuando se requiera, no establecida; entre otras),

d. **Complemento**: Todos los detalles necesarios para entender claramente el propósito del control (detalles como las evidencias, como se hace la actividad, entre otros)

Caracterización de Controles

Una vez descrito el control, para poder analizarlo se debe completar la información de este, mediante la asignación de unas características establecidas, las cuales se dividen en dos grupos de acuerdo con su naturaleza, los atributos de eficiencia, sobre los cuales se calificará el control, y los atributos informativos que permitirán conocer el entorno del control y complementar la información que permita hacer un análisis cualitativo de este. Los atributos informativos no tienen incidencia en la calificación de un control.

Clasificación de acuerdo con los atributos de eficiencia: Para clasificar los controles según sus atributos de eficiencia deben ser analizados a través de 2 tipologías; en primer lugar, debe analizarse en qué fase del ciclo de procesos se aplica el control, esto permite determinar si el control es preventivo, detectivo o correctivo (tipo de control); la segunda tipología indica la forma como se ejecuta o implementa el control, si es manual o automático (forma de implementación).

Acorde con lo anterior se tienen las siguientes clasificaciones de acuerdo con el tipo de control:

- **Preventivo:** Se aplica el control en la entrada de los procesos (antes de que se realice la actividad crítica que genera el riesgo) y se enfocan en las causas del riesgo, de tal forma que previenen su materialización con lo cual reducen la probabilidad de ocurrencia.
- **Detectivo:** El control se ejecuta durante la realización del proceso (mientras se realiza la actividad crítica que genera el riesgo) de forma que al detectar una desviación no permite continuar, con lo cual se generan reprocesos. Los controles detectivos se enfocan en evitar que el riesgo se materialice al no permitir que se avance con una actividad, estos reducen la probabilidad de ocurrencia.
- **Correctivo:** Un control es correctivo cuando se ejecuta a partir de las salidas del proceso (después de realizar la actividad crítica que produce el riesgo), es decir que aplican una vez el riesgo se ha materializado, y su propósito es reducir el impacto negativo que genera dicha materialización.

De acuerdo con la forma como se implementa o ejecuta el control

- **Automático:** Corresponde a controles que son realizados por sistemas y/o aplicativos sin que intervengan personas en su realización.
- **Manual:** Aquellos ejecutados por personas, con lo cual tienen implícito el error humano.

Valoración de Controles

Una vez definidos los controles, para determinar su peso en la mitigación del riesgo asociado se deben tener en cuenta sus atributos de eficiencia, es decir el tipo de control y la forma como se

PÚBLICA

ejecuta o implementa, con lo que se obtendrá la calificación del riesgo residual**.** A continuación, se relaciona el peso de cada atributo:

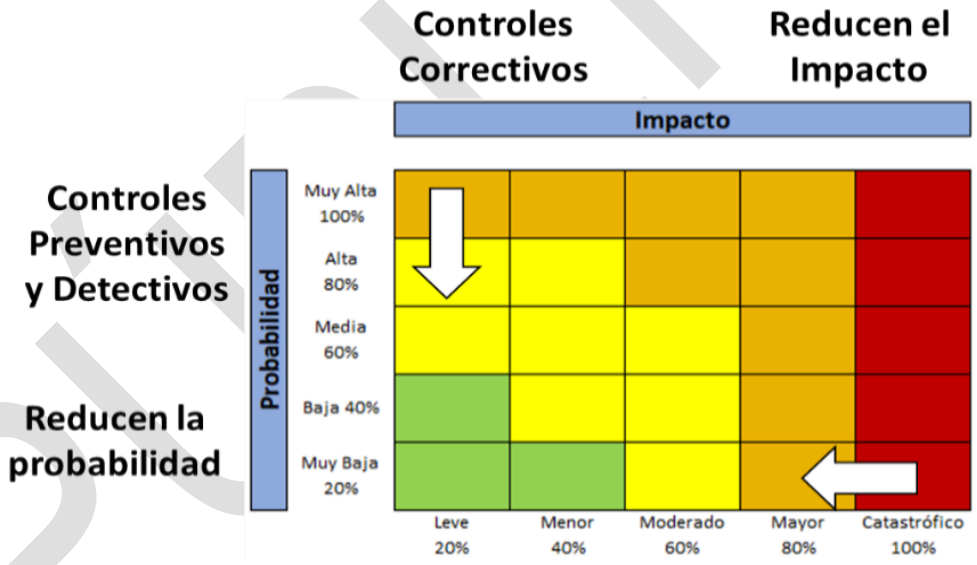
Tabla 52. Ponderación atributos de eficiencia de controles ambientales

CARACTERÍSTICAS		PESO
Tipo	Preventivo	**25%**
	Detectivo	**15%**
	Correctivo	**10%**
Implementación	Automático	**25%**
	Manual	**15%**

Fuente: Adaptado de la Guía para la administración del riesgo y diseño de controles en entidades públicas del Departamento administrativo de la Función Pública -DAFP

De acuerdo con el tipo de control se establecerá el eje de la matriz de riesgos (probabilidad o impacto) en el cual se moverá. Si el control reduce el impacto la ubicación del riesgo se moverá a la izquierda, si por el contrario reduce la probabilidad se moverá hacia abajo, en la siguiente imagen se muestra la aplicación de lo anterior.

Imagen 20. Movimiento de los riesgos en la matriz de calor acorde al tipo de control



Fuente: Adaptado de la Guía para la administración del riesgo y diseño de controles en entidades públicas del DAFP – V5 y V6.

Clasificación de acuerdo con los atributos informativos: Con estas características se busca complementar la información de los controles estableciendo la formalidad del control para conocer su entorno, de acuerdo con lo anterior se podrá establecer, si está documentado, su frecuencia de ejecución y si se cuenta o no con evidencias de esta.

Tabla 53. Atributos informativos controles de riesgo ambiental

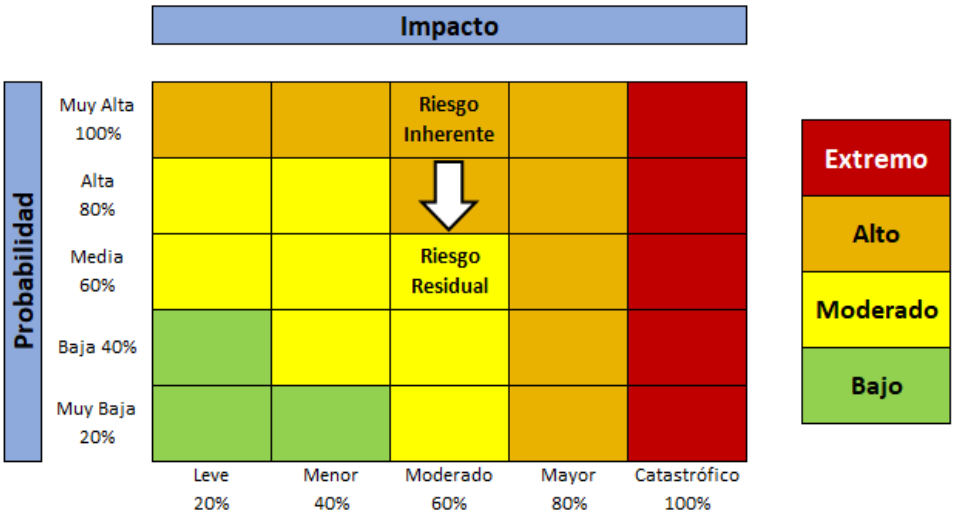
ATRIBUTO	CLASIFICACIÓN	DESCRIPCIÓN
Documentación	Documentado	El control se encuentra descrito en un documento del proceso (procedimientos, guías, manuales, operativos, lineamientos, etc.)
	Sin documentar	El control si bien se ejecuta no se encuentra descrito en ningún documento
Frecuencia	Continua	El control se ejecuta cada vez que se realiza la actividad crítica que genera el riesgo.
	Aleatoria	El control se ejecuta de manera aleatoria a la realización de la actividad que genera el riesgo.
Evidencia	Con registro	Cuando se ejecuta el control se genera un registro que permite evidenciar su aplicación.
	Sin registro	Cuando se ejecuta el control no se genera un registro y por lo tanto no se puede evidenciar su aplicación.

Nivel de Riesgo Residual

El nivel de riesgo residual es la calificación del riesgo que se obtiene una vez aplicados los controles, la cual dependerá de la valoración de los controles asociados a este. Para calcular el riesgo residual se deberá calcular de forma acumulativa, es decir se calcula el valor de probabilidad o impacto de acuerdo con el peso del primer control y sobre el resultado se aplicará el segundo control, así sucesivamente dependiendo del número de controles.

Con los valores de probabilidad e impacto residuales, se procede a ubicar el riesgo en el mapa de calor teniendo en cuenta las mismas indicaciones que en la etapa de análisis. Como se observa a continuación una vez aplicados los controles el riesgo bajó dos niveles en su probabilidad, quedando en una zona de riesgo Moderado.

Imagen 21. Riesgo residual mapa de calor



6.5 Tratamiento de Riesgos

Cuando la calificación del riesgo residual sea moderado, alto o extremo el líder o responsable de proceso debe implementar estrategias que permitan combatir los riesgos evitando así que se materialice. Lo anterior no quiere decir que cuando un riesgo se encuentre en nivel bajo no pueda ser tratado.

Para realizar el tratamiento de riesgos se tendrán tres estrategias posibles, que serán evitar, transferir o mitigar el riesgo.

Evitar: Consiste en que posteriormente a determinar el nivel de riesgo residual, se decide eliminar la actividad crítica que provoca el riesgo, con lo cual se eliminaría o evitaría el riesgo. Sin embargo, mientras no se realicen los ajustes pertinentes al proceso y la actividad siga vigente, el riesgo deberá ser gestionado a través de alguna de las otras estrategias de tratamiento.

Transferir: Consiste en trasladar el riesgo a un tercero, bien sea tercerizando el proceso o a través de una póliza de seguro. Esta estrategia aplicará únicamente para aquellos riesgos cuyo impacto sea económico, en tal caso se deberá hacer un análisis basado en los otros tipos de impacto para definir si el riesgo persiste en la entidad.

Mitigar: Consiste en implementar acciones para reducir el nivel de riesgo. En el marco de esta estrategia, se pueden establecer dos escenarios siempre enmarcados en un plan de tratamiento que contemple: actividades definidas, responsables, fechas de inicio y fin, periodicidad (para actividades que se repitan durante un periodo de tiempo), evidencias y seguimiento, lo cuales pueden ser:

- **Implementar nuevos controles:** Como su nombre lo indica esta estrategia consiste en generar nuevos controles dentro del proceso que contribuyan a mejorar la calificación del riesgo residual, atacando la probabilidad de ocurrencia del riesgo o su impacto.

- **Realizar actividades complementarias de mitigación de riesgos:** Consiste en la realización de actividades que contribuyan a evitar la materialización del riesgo, que pueden ser, seguimientos, actividades de fortalecimiento al recurso humano, verificaciones, entre otras. Es importante recordar que estas actividades deben estar en el marco de un plan de trabajo y contar con las características antes mencionadas.

6.6 Monitoreo y Revisión

El monitoreo y revisión de los riesgos, controles existentes y planes de tratamiento, se realiza por parte del profesional de la Sede de la Dirección General y referentes ambientales, teniendo en cuenta la periodicidad y fechas de cumplimiento establecidas, registrando los resultados de cada una de las actividades desarrolladas en la Matriz de Riesgos, así como el cargue de cada uno de los soportes correspondientes a los controles en el repositorio.

PUBLICA

Una vez las regionales realicen el reporte de cumplimiento de sus planes de tratamiento, los profesionales ambientales de la Dirección Administrativa realizan la revisión y validación de esta información, con el fin de reportar la medición cuatrimestral de la gestión del riesgo a través del indicador.

El reporte de cumplimiento de las acciones de los planes de tratamiento por parte de las regionales se debe realizar dentro de los primeros 5 días hábiles siguiente a la fecha de corte. De igual manera el avance en la gestión de los riesgos se revisa semestralmente por la alta dirección en la revisión por la dirección.

Por último, el reporte de la materialización de riesgos y ejecución de controles existentes se debe realizar por parte de los profesionales o referentes ambientales, realizando el cargue de las evidencias de cumplimiento en el repositorio del Eje Ambiental, lo anterior, de acuerdo con las indicaciones impartidas por la Dirección Administrativa.

7. GESTION DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION, CIBERSEGURIDAD, Y CONTINUIDAD DE LA OPERACIÓN.

La gestión de riesgos de Seguridad y Privacidad de la Información, ciberseguridad, y Continuidad de la Operación, le permite al ICBF establecer el alcance para realizar una identificación, análisis, valoración, manejo o tratamiento a los riesgos que puedan generar afectación al cumplimiento de los objetivos de sus procesos, contribuyendo en la toma de decisiones con el fin de prevenir la materialización de estos. La presente guía tiene como referencia las siguientes buenas prácticas: Estándar Internacional **ISO 31000:2018**, Guía para la administración del riesgo y el diseño de controles en entidades pública – **DAFP**, Política Nacional de Seguridad Digital - **CONPES 3854 de 2016**, Modelo de Seguridad y Privacidad de la Información – **MINTIC** y políticas propias de la Entidad (**SIGE**).

7.1. Objetivos

- Propender por la confidencialidad, integridad y disponibilidad de la información que maneja la Entidad
- Identificar, analizar, valorar, manejo o planes de tratamiento, monitorear controles existentes y evaluar los riesgos residuales de los Riesgos de Seguridad y Privacidad de la Información, ciberseguridad, y Continuidad de la Operación del ICBF identificados en la vigencia
- Proteger los activos de información identificados como críticos por la entidad
- Brindar orientaciones en temas referentes a la gestión de riesgos de Seguridad de la Información, ciberseguridad, y Continuidad de la Operación en sus fases de establecimiento del alcance, contexto y criterios del proceso, identificación, análisis y valoración de riesgos, tratamiento y evaluación del riesgo residual.
- Minimizar el impacto de los incidentes de seguridad y privacidad de la información, ciberseguridad y continuidad de la operación

PUBLICA

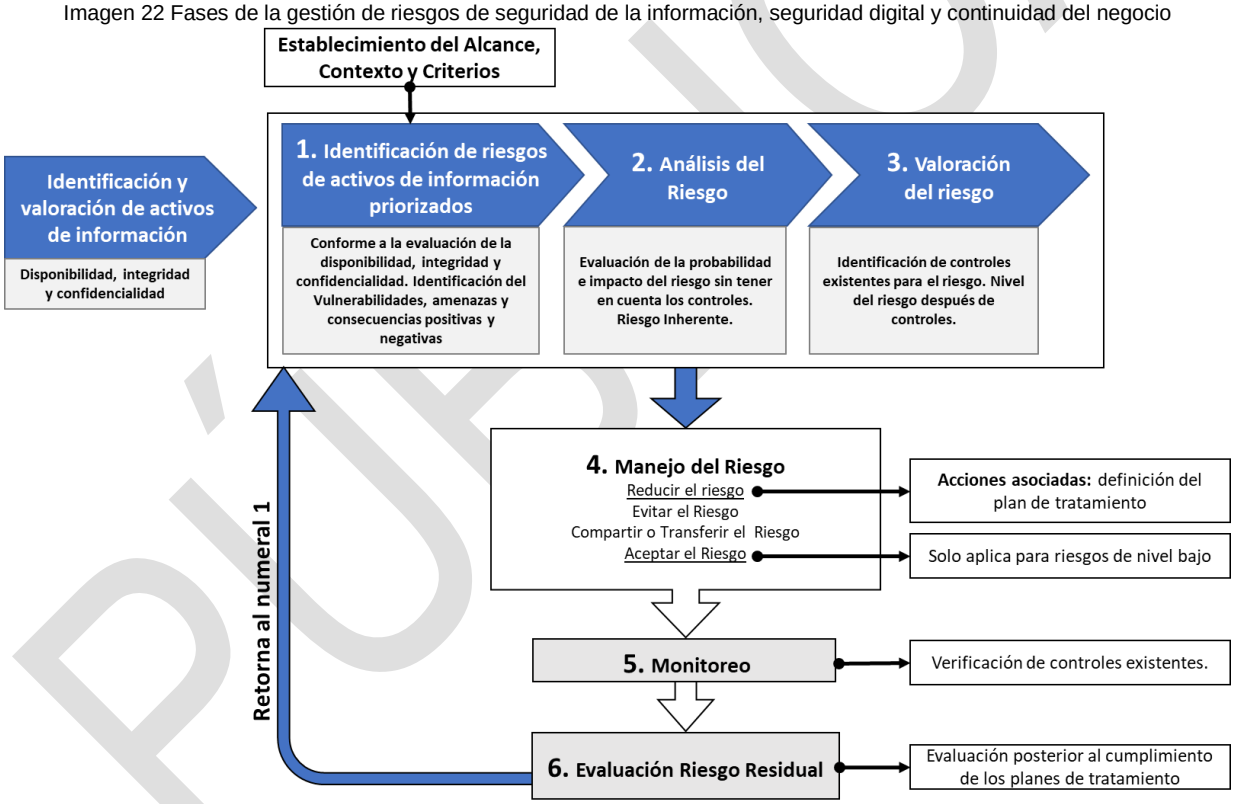
7.2. Condiciones Generales

7.2.1. Esta guía deberá ser tomada como base, para identificar riesgos de Seguridad y Privacidad de la información, ciberseguridad, y Continuidad del de la Operación

7.2.2. Para una adecuada gestión de riesgos es importante tener un análisis previo de la entidad considerando aspectos generales como la Misión, Visión, Objetivos y Planeación Institucional, además de conocer y comprender el modelo de operación por procesos considerando sus caracterizaciones y actividades principales.

7.2.3. Para la gestión de riesgos de Seguridad y Privacidad de la información, ciberseguridad, y Continuidad de la Operación en el ICBF se contemplan las siguientes fases: identificación de riesgos de activos de información priorizados, análisis del riesgo, valoración del riesgo, manejo del riesgo (tratamiento del riesgo), monitoreo y evaluación del riesgo residual (en dado caso si el riesgo no es mitigado o llevado a un nivel bajo, es necesario generar nuevamente el tratamiento).

Imagen 22 Fases de la gestión de riesgos de seguridad de la información, seguridad digital y continuidad del negocio



7.2.4. Los procesos en la Sede de la Dirección General y las Regionales deben elaborar un acta en la cual se consigne los resultados de la identificación, análisis, valoración y manejo (tratamiento del riesgo) de los riesgos de Seguridad y Privacidad de la información, ciberseguridad y Continuidad de la operación. El acta deberá contener el ID de los riesgos, proceso, nombre del activo de información afectado, tipo de activo afectado, descripción del riesgo, tipo de riesgo, vulnerabilidades, amenazas, consecuencias negativas, consecuencias positivas, nivel y los planes de tratamiento con las actividades, fechas de cumplimiento,

PÚBLICA

responsables y evidencia. Por otra parte, el acta deberá ser firmada por los líderes o responsables de los procesos o los directores regionales.

7.2.5. Posterior al registro de la información en Suite Visión Empresarial y revisión metodológica por parte del Equipo de Seguridad de la Información, los líderes o responsables de los procesos en la Sede de la Dirección General y/o directores(as) de las Regionales deberán emitir un memorando de la aprobación de estos riesgos dirigido al director(a) de la Dirección de Información y Tecnología cómo líder del Eje de Seguridad de la Información, anexando el acta relacionada en el numeral 7.2.4. En este memorando se debe relacionar la aceptación de los riesgos conforme a los resultados descritos en el acta y registrados en el sistema.

7.2.6. Para los riesgos identificados en el proceso de Gestión de Tecnología de la información, los subdirectores de la Subdirección de Sistemas Integrados de Información y Subdirección de Recursos Tecnológicos enviarán un memorando de aprobación dirigido al director de la Dirección de Información y Tecnología como líder del Eje de Seguridad de la Información.

7.2.7. Para facilitar el ejercicio de identificación, análisis, valoración y definición de las actividades de los planes de tratamiento se establece el formato F3.G3.MI “Formato Matriz de Riesgos Sistema de Gestión de Seguridad de la Información” como herramienta de recolección de la información de los riesgos, la cual podrá ser usada para la generación del ID, desarrollar las mesas de trabajo en los casos que aplique y solicitudes para el registro de nuevos riesgos en el sistema de información.

7.2.8. El Sistema de información SUITE VISION EMPRESARIAL es el establecido para la Gestión de Riesgos, en este se registrará la información de la identificación, análisis, valoración y manejo, así mismo se realizará el seguimiento a los planes de tratamiento y monitoreo de los controles existentes o reporte de materializaciones. La información registrada en este sistema será la oficial para la gestión de los riesgos y presentación de soportes ante auditorías internas y externas.

7.2.9. Para el registro de un riesgo nuevo en el sistema de información el Promotor EPICO o Ingeniero Regional deberá remitir la solicitud de creación en el sistema al Gestor de Riesgos de Seguridad de la Información mediante correo electrónico, en el cual deberán relacionar el identificador, responsable, gestor, descripción, clase de riesgo, objetivo del proceso, área organizativa, causas y consecuencia, para que este proceda con el registro de la información. Cuando finalice, notificará al Promotor EPICO o ingeniero regional para que continúe con el registro de la información en el sistema, hasta llevar el riesgo a la fase de monitoreo. Posterior a esto se deberá dar cumplimiento a las condiciones generales 7.2.4 y 7.2.5.

7.2.10. Cuando producto de realizar el ejercicio anual de la identificación, análisis, valoración, manejo del riesgo, evaluación del riesgo residual o por alguna otra situación, se requiera ajustar la información de los riesgos ya registrados en el sistema de información, se deberá solicitar a través de esta herramienta volver a la fase en la que se van a realizar las modificaciones, anexando en la solicitud la justificación de porque se requiere el cambio. Posterior a esto se deberán remitir los soportes de la aprobación siguiendo lo definido en las condiciones generales 7.2.4 y 7.2.5. Las demás solicitudes relacionadas con errores en el registro de la información se solicitarán igualmente mediante el sistema, pero se deberá indicar el error a corregir y deberá corresponder a la información registrada en el acta de identificación ya aprobada.

7.2.11. Para cambios de responsable o gestor, el líder o responsable del proceso deberá realizar solicitud mediante correo electrónico al Director de Información y Tecnología como Líder del Eje de Seguridad de la Información con copia al Gestor de Riesgos, indicando el motivo por

PÚBLICO

el cual se requiere el cambio. Posterior a la autorización, el Gestor de Riesgos de Seguridad de la Información procederá a realizar el cambio en el sistema.

7.2.12. Las solicitudes de modificaciones de la descripción, fechas de cumplimiento o algún otro cambio de las actividades de los planes de tratamiento para los riesgos de Seguridad de la Información, ciberseguridad, y continuidad de la Operación, deberán ser realizadas por el líder o responsable del proceso y dirigidas al Director de Información y Tecnología con copia al Gestor de Riesgos de Seguridad de la Información a través de correo electrónico, antes de la fecha de finalización de la actividad y justificando la necesidad del cambio. Es de anotar, que dichas solicitudes se podrán realizar hasta el 31 de agosto de cada vigencia. Lo anterior, con el fin de que se evalué las modificaciones y se tome las acciones correspondientes para ajustar la información en el sistema. Cuando la justificación del cambio de las actividades de los planes de tratamiento esté relacionada con temas presupuestales o temas de gestión con otras dependencias, se podrán ajustar hasta el mes de noviembre indicando el motivo y las gestiones realizadas a la fecha.

7.2.13. El líder o responsable del proceso deberá informar los nuevos riesgos que sean identificados durante la vigencia al Director de Información y Tecnología con copia al Gestor de riesgos de Seguridad de la Información, a través de correo electrónico para su validación, Una vez revisado y avalado el nuevo riesgo por el Líder del Eje de Seguridad de la Información, el Promotor EPICO de los procesos de la SDG o el referente de seguridad de la Información de la Regional deberá incluir el riesgo en el sistema de información siguiendo la condición general 7.2.9 y generando los soportes de acuerdo a los numerales 7.2.4. y 7.2.5. En ningún caso se podrá inactivar en SVE un riesgo de seguridad y privacidad de la información, ciberseguridad y continuidad de la operación, a menos que el activo de información asociado a este, desaparezca del proceso, adicionalmente para efectos de documentación deberá remitirse un memorando firmado por los líderes o responsables de los procesos o los directores regionales, dirigido al Director de Información y Tecnología

7.2.14. Los colaboradores del ICBF deberán informar al gestor de Riesgos de Seguridad de la Información mediante correo electrónico cuando consideren que un evento propio puede ser tratado como Riesgo de Seguridad y Privacidad de la Información, ciberseguridad, y de Continuidad de la Operación, con el fin de que se evalué, analice y realice la identificación del riesgo si corresponde conforme a lo establecido en el numeral 7.2.9.

7.2.15. El monitoreo de los controles existentes se realizará conforme al cronograma que defina el Gestor de Riesgos posterior a la fase de valoración de riesgos. En esta actividad, los Gestores de los Riesgos registrados en el Sistema de Información SVE, deberán reportar a través de este el análisis y evidencias del cumplimiento de los controles, indicando si el riesgo se ha materializado y cualquier otra observación que aporte a su seguimiento.

7.2.16. Cuando se materialice un riesgo de seguridad de la información, ciberseguridad y continuidad de la Operación, los propietarios o responsables de los procesos deberán reportarlo siguiendo lo definido en el P5.GTI “Procedimiento gestión de incidentes de seguridad y privacidad, de la información”. Cuando se haya finalizado con las actividades del procedimiento, el Promotor EPICO o Ingeniero Regional deberá convocar una mesa de trabajo, en la cual participarán el Gestor de Riesgos de Seguridad de la Información, el Gestor de Incidentes de Seguridad de la Información y los colaboradores relacionados en la materialización de incidente. En esta mesa de trabajo, se deberán revisar si es necesario identificar un nuevo riesgo o reformular uno existente o establecer actividades de tratamiento que propendan por mitigar una nueva materialización. Lo anterior, deberá ser documentado en un acta por parte del Promotor EPICO o Ingeniero Regional, remitiendo copia al Gestor

de Riesgos de Seguridad de la Información.

7.2.17. Cuando resultado de la materialización de un riesgo se requiera identificar uno nuevo, se deberá cumplir con lo definido en las condiciones general 7.2.9. y 7.2.13. En los casos que se vaya a reformular un riesgo existente, se seguirá lo establecido en el numeral 7.2.10.

7.2.18. Los controles existentes que se identifiquen para los riesgos de seguridad de la información deben orientarse a mitigar vulnerabilidades, amenazas o consecuencias asociadas a este. Igualmente, los controles deben identificarse conforme al tipo de activo relacionado en el riesgo, por ejemplo, para el tipo “Físico – Electrónico” deben asociarse los controles tanto para la parte física como electrónica.

7.2.19. En la fase de valoración de riesgos se debe procurar por identificar todos los controles que aporten de manera conveniente a la calificación del riesgo después de controles, es decir a mitigar la probabilidad de que se materialice o reducir el impacto en caso de que se presente.

7.2.20. Los controles existentes que se identifiquen deben abarcar todas las causas del riesgo (vulnerabilidades o amenazas), en caso de no hacerlo este deberá pasar a tratamiento para generar las actividades que permitan el control o mitigación de las faltantes.

7.2.21. El ejercicio de identificación de riesgos de Seguridad y Privacidad de la información, ciberseguridad, y Continuidad de la Operación se realizará de forma anual, revisando con los Líderes o Responsables de los Procesos y los Directores Regionales, la totalidad de los riesgos, con el fin de determinar si es necesario realizar ajustes sobre estos. Para lo anterior, deberá darse cumplimiento a las condiciones generales, 7.2.4, 7.2.5, 7.2.9 y 7.2.10.

7.3. Identificación de riesgos de activos de información priorizados

7.3.1. Establecimiento del alcance, contexto y criterios

El Instituto Colombiano de Bienestar Familiar – ICBF, es un establecimiento público, es decir, es una entidad dotada de personería jurídica, autonomía administrativa y patrimonio propio; creada mediante la Ley 75 de 1968, es la entidad del Estado Colombiano con casi medio siglo de experiencia en la protección integral de los niños, niñas, adolescentes, y de acuerdo con la nueva estructura de la entidad, desde el 2020 el ICBF fortalece las capacidades de los jóvenes y las familias como actores clave de los entornos protectores y principales agentes de transformación social.

El ICBF brinda atención a niños, niñas, adolescentes, jóvenes y familias, especialmente aquellos en condiciones de amenaza, inobservancia o vulneración de sus derechos. Desde el año 2011 se encontraba adscrito al Sector de la Inclusión Social y la Reconciliación, y a partir de junio de 2023, mediante el Decreto 1074, fue adscrito al Sector Administrativo de Igualdad y Equidad, en cabeza del Ministerio de Igualdad y Equidad.

El Instituto cuenta con 33 regionales, ubicadas en los Departamentos y en el Distrito Capital y 216 Centros Zonales que hacen presencia en el ámbito municipal y local en todo el territorio nacional; llegando a más de ocho (8) millones de colombianos con el servicio público de bienestar familiar, a través de sus programas y estrategias de atención. Considerando esta configuración política, administrativa, social y geográfica del ICBF en el presente documento se relaciona el análisis del contexto externo e interno, el cual cuenta con la siguiente estructura metodológica: aplicación de las perspectivas PESTA (política, económica, social, tecnológica, ambiental “medioambiental”) para analizar el contexto externo, articulado e integrado con los aspectos de la metodología DOFA (debilidades, oportunidades, fortalezas y amenazas -internas y externas-) para tener una visión holística y global de la Entidad y su entorno.

PUBLICA

Contexto del proceso: Se deben determinar las características o aspectos esenciales del proceso y sus interrelaciones, teniendo en cuenta el nuevo modelo de operación por procesos, donde se tienen en cuenta los siguientes factores:

- ✓ Diseño del proceso
- ✓ Interacción con otros procesos
- ✓ Procedimientos asociados
- ✓ Responsables del proceso
- ✓ Comunicación entre los procesos
- ✓ Activos de seguridad digital
- ✓ Gestión de conocimiento

7.3.1.1 Roles y Responsabilidades

Para iniciar la fase de identificación de riesgos como primera medida se establecen los siguientes roles con sus responsabilidades:

Rol	Responsabilidad
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.

7.3.2. Codificación y Redacción de riesgos de Seguridad y Privacidad de la información, ciberseguridad y Continuidad de la Operación

Como paso inicial para la identificación de riesgos de seguridad y privacidad de la información, ciberseguridad y continuidad de la Operación, se debe validar cuales son los activos priorizados del inventario de activos de información. Así mismo, se deben evaluar los diferentes aspectos de la entidad como infraestructura física, 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 los objetivos establecidos para la misma.

Para cada riesgo se debe generar un identificador de la siguiente forma:

- Dos últimas cifras del año de la identificación del riesgo al inicio de la codificación.
- Sigla del proceso dueño del riesgo.
- Sigla de la Regional o Sede que identifica el riesgo.
- Número consecutivo del riesgo conforme al año.

Por ejemplo, el Id del riesgo 24GTIATL1, correspondería al primer riesgo identificado para el proceso de Gestión de Tecnología e Información en la regional Atlántico en la vigencia 2024.

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 atributo(s) es(son) afectado(s) (Confidencialidad, Integridad, Disponibilidad).

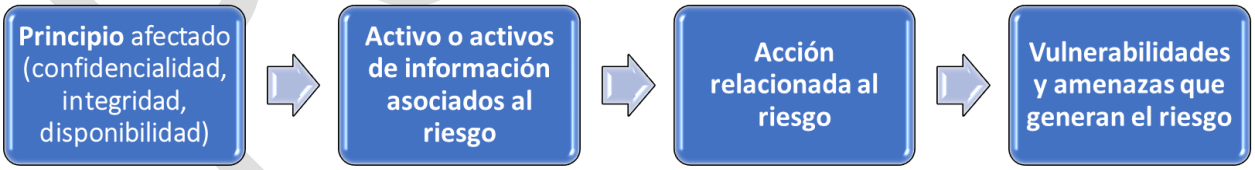
Las preguntas claves para la identificación del riesgo permiten determinar:

- ¿QUÉ PUEDE SUCEDER? Identificar la afectación del cumplimiento del objetivo estratégico o del proceso según sea el caso.
- ¿CÓMO PUEDE SUCEDER? Establecer las causas a partir de los factoresdeterminados en el contexto.
- ¿CUÁNDO PUEDE SUCEDER? Determinar de acuerdo con el desarrollo delproceso.
- ¿QUÉ CONSECUENCIAS TENDRÍA SU MATERIALIZACIÓN? Determinar losposibles efectos por la materialización del riesgo.

En la descripción del riesgo se deben tener en cuenta las respuestas a las preguntas mencionadas anteriormente.

Para la redacción de un riesgo se debe tener en cuenta la siguiente estructura:

Imagen 23 Estructura de redacción de un riesgo de seguridad y privacidad de la información, ciberseguridad, y continuidad de la Operación



Ejemplos:

- Pérdida de integridad de (activo o activos de información), debido a (actividad/situación+ vulnerabilidades y amenazas)

PÚBLICA

- Pérdida de integridad de la base de datos de nómina, debido a la modificación de información sin autorización por la falta de políticas de control de acceso, contraseñas sin protección y mecanismos de autenticación débil.

- Pérdida de confidencialidad de (activo o activos de información relacionados en el riesgo), debido a (actividad/situación+ vulnerabilidades y amenazas).

- Pérdida de confidencialidad de las historias de atención, debido a la conexión de computadores utilizados por los colaboradores para realizar trabajo en casa, a redes personales o públicas que no cuentan con controles suficientes para evitar ataques de malware, phishing u otro.

- Pérdida de disponibilidad del (activo o activos de información), debido a (actividad/situación+ vulnerabilidades y amenazas).

Pérdida de disponibilidad de equipos de cómputo y dispositivos de red, debido a cortes de energía no controlados, por fallas en la UPS y/o planta eléctrica que no se les han realizado los mantenimientos preventivos y correctivos correspondientes

Para el caso de que por una misma acción se puedan afectar dos o tres principios de seguridad de la información (confidencialidad, integridad y disponibilidad), se podrán agrupar en un solo riesgo como se muestra a continuación:

Pérdida de confidencialidad, integridad y o disponibilidad de la aplicación SIM debido a interceptación de tráfico por el uso de protocolos no seguros (TLS y SSL), desactualización tecnológica y ataque informáticos.

La falta de apropiación en temas referentes a la seguridad de la información o la ausencia de controles (vulnerabilidades) puede ser aprovechadas por una amenaza causando la materialización de un riesgo (incidente), por lo que es preciso identificar lo siguiente:

- Proceso
- Dueño o responsable del riesgo
- Activos y/o servicios
- Riesgo
- Clasificación del riesgo
- Fuentes, Causas, Amenazas y vulnerabilidades

7.3.3. Identificación de Activos de Información Priorizado

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 nuevo modelo de operación por procesos. Mediante la identificación y formalización de un inventario de activos de seguridad de la 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 la cual puede consultarse en el portal web.

PUBLICA

Los activos de información priorizados son los que pasan a evaluación de riesgos porque finalizada su identificación y valoración cumplen con alguna de las siguientes premisas:

- Cuando en alguno de los criterios de confidencialidad, integridad y disponibilidad su calificación sea igual a tres (3). En este caso, deberá edificarse un riesgo del activo de información asociado con el principio que haya quedado con esa valoración.
- Todos los activos que hayan quedado con un nivel de importancia alta deberán pasar a identificación y evaluación de riesgos.

7.3.4. Identificación de consecuencias positivas y negativas.

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.

Adicionalmente se deben considerar las consecuencias positivas y negativas, teniendo en cuenta la estandarización que se relaciona a continuación.

Tabla 54 Clasificación de consecuencias negativas

Consecuencias negativas
Pérdidas financieras
Pérdida reputacional
Incumplimientos legales
Daños a la Infraestructura Física
Daños a la Infraestructura Tecnológica
Llamados de Atención
Sanciones
Reprocesos
Interrupción de la Operación o del Servicio

Consecuencias Positivas
Adquisición de conocimiento
Optimización de recursos económicos
Optimización de recursos humanos
Optimización de recursos tecnológicos
Optimización de procesos
Optimización en la Mejora de la reputación
Reducción de la exposición a amenazas
Optimización de Recursos
Reducción Pérdidas financieras
Optimización en el Cumplimiento normativo legal
Aumento de confianza de las partes interesadas
Aumento de la resiliencia organizacional

7.3.5. Clasificación riesgos

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 y privacidad 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

PÚBLICA

sus consecuencias[4] que afecta la confidencialidad, integridad o disponibilidad de la información.

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

- Riesgos de Continuidad de la Operación: son aquellos riesgos que involucran alguna afectación, faltas o fallas en la disponibilidad de las personas, proveedores, información, sistemas o infraestructura tecnológica que soporta los servicios críticos que brinda la entidad. A continuación, se enuncian algunos ejemplos de aquellos escenarios que pueden generar la identificación de un riesgo de continuidad de la operación:

    a. Fallo en el fluido eléctrico.
    b. Fallo en el canal de comunicaciones.
    c. Fallo físico en el servidor de almacenamiento.
    d. Fallo en el centro de cableado.
    e. Fallo en el medio de conexión entre centro de cableado.

7.4. Análisis del Riesgo

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 materializado sobre en 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 conocimientodel dueño del riesgo).
- Datos Externos (Datos oficiales reportados por entes regulatorios y competentes quese relacionen con riesgos que afecten el contexto externo).

Este proceso se hace partiendo de la experiencia de los funcionarios y el acompañamiento metodológico del Gestor de Riesgos de Seguridad de Información. Se puede realizar el análisis de riesgos utilizando una o varias de las siguientes técnicas:

- Entrevistas
- Cuestionarios
- Listas de chequeo
- Tormenta de ideas
- Grupo de expertos
- Opinión de expertos

[4] Tomado de (ISO/IEC 27000)

PÚBLICA

En la fase de análisis debe realizarse la calificación de la probabilidad e impacto, siguiendo los siguientes cuadros:

Tabla 55 Probabilidad

PROBABILIDAD	CONCEPTO	DESCRIPCIÓN
100%	Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año
80%	Alta	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5000 veces por año.
60%	Media	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año
40%	Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 23 veces por año
20%	Muy baja	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año.

Tabla 56 Impacto

Impacto	Afectación Económica	Reputacional
Catastrófico 100%	Mayor a 500 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país
Mayor 80%	Entre 100 y 500 SMLMV	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal.
Moderado 60%	Entre 50 y 100 SMLMV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos.
Menor 40%	Entre 10 y 50 SMLMV	El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, de junta directiva y accionistas y/o de proveedores.
Leve 20%	Afectación menor a 10 SMLMV	El riesgo afecta la imagen de algún área de la organización.

Aunque inicialmente la mayoría de los riesgos serán analizados de forma cualitativa, a medida que el proceso de gestión de riesgos madura, obtendrá datos relevantes que permitirán hacer un análisis cuantitativo con un mayor nivel de exactitud en la calificación de probabilidad, impacto y eficacia de controles.

A continuación, se mencionan 6 aspectos que se deben tener en cuenta para realizar un adecuado análisis de riesgo:

- Tener un inventario de activos de información en el cual se hayan asignado por cada principio (confidencialidad, integridad y disponibilidad) un valor conforme a su importancia.
- Investigar cada uno de los activos priorizados y tener una relación de las amenazas y vulnerabilidades que le pueden afectar.
- Determinar las actividades o situaciones que conllevan a la materialización de riesgos y determinar cuántas veces se puede ejecutar o presentar esta en el año.
- Determinar el potencial de afectación que tendría un riesgo sobre la entidad en caso de materializase.

PÚBLICA

El análisis de riesgos tiene como objeto priorizar los riesgos identificados de acuerdo con el nivel inherente (criticidad) obtenido, evaluando y determinando la probabilidad, el impacto de acuerdo con las vulnerabilidades y amenazas identificadas sin tener en cuenta los controles existentes.

Imagen 24 Análisis del Riesgo Inherente - Probabilidad por Impacto

		Impacto				
Probabilidad	Muy Alta 100%	Alto (Muy alta - Leve)	Alto (Muy Alta - Menor)	Alto (Muy Alta - Moderado)	Alto (Muy Alta - Mayor)	Extremo (Muy Alta - Catastrófico)
	Alta 80%	Moderado (Alta - Leve)	Moderado (Alta - Menor)	Alto (Alta - Moderado)	Alto (Alta - Mayor)	Extremo (Alta - Catastrófico)
	Media 60%	Moderado (Media - Leve)	Moderado (Media - Menor)	Moderado (Media - Moderado)	Alto (Media - Mayor)	Extremo (Media - Catastrófico)
	Baja 40%	Bajo (Baja - Leve)	Moderado (Baja - Menor)	Moderado (Baja - Moderado)	Alto (Baja - Mayor)	Extremo (Baja - Catastrófico)
	Muy Baja 20%	Bajo (Muy Baja - Leve)	Bajo (Muy Baja - Menor)	Moderado (Muy Baja - Moderador)	Alto (Muy Baja - Mayor)	Extremo (Muy Baja - Catastrófico)
		Leve 20%	Menor 40%	Moderado 60%	Mayor 80%	Catastrófico 100%
	Escala de valoración:	Extremo	Alto	Moderado	Bajo	

7.5. Valoración del riesgo

En esta fase se realiza la Identificación de controles existentes para la mitigación del riesgo, debiendo asociar 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 deben mitigarlas.

Por lo anterior, debe determinarse 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 conforme a los siguientes criterios:

7.5.1. Diseño del control:

Los criterios de evaluación del control con relación al diseño son:

Tabla 57 Calificación diseño del control

	Calificación		
Criterios	Fuerte (3)	Moderado (2)	Débil (1)
Responsable asignado	Cuando cumple con todos los criterios establecidos para evaluar el diseño del control	Cuando no cumple con uno o tres de los criterios establecidos para evaluar el diseño del control	Cuando no cumple con 4 o ninguno de los criterios establecidos para evaluar el diseño del control
Periodicidad definida			
Descripción de cómo se ejecuta			
Está documentado			
Que pasan con las observaciones o desviaciones			
Existen evidencias de la ejecución			

7.5.2. Ejecución del control:

Los criterios de evaluación del control con relación a su ejecución son:

Tabla 58 Calificación ejecución del control

Calificación	Criterio
Fuerte (3)	El control se ejecuta de manera consistente conforme a la periodicidad definido y cuenta con todas las evidencias correspondientes.
Moderado (2)	El control se ejecuta algunas veces por parte del responsable y cuenta con algunas evidencias.
Débil (1)	El control no se ejecuta por parte del responsable y no se tiene evidencia del cumplimiento.

7.5.3. Fortaleza de los controles:

Para calcular la efectivad de los controles se realiza la multiplicación entre el valor dado al diseño del control por la ejecución de mismo, como se indica en la siguiente tabla:

Tabla 59 Cálculo de diseño vs ejecución del control efectividad del control

Diseño		Ejecución		(Diseño x Ejecución)
Fuerte	3	Fuerte	3	9
Fuerte	3	Moderado	2	6
Fuerte	3	Débil	1	3
Moderado	2	Fuerte	3	6
Moderado	2	Moderado	2	4
Moderado	2	Débil	1	2
Débil	1	Fuerte	3	3
Débil	1	Moderado	2	2
Débil	1	Débil	1	1

De lo anterior se determina si un control es efectivo, moderadamente efectivo o poco efectivo como se muestra en las siguientes tablas:

Tabla 60 Efectividad de Controles

DISEÑO	Fuerte (3)	Poco efectivo (3)	Moderadamente efectivo (6)	Efectivo (9)
	Moderado (2)	Poco efectivo (2)	Moderadamente efectivo (4)	Moderadamente efectivo (6)
	Débil (1)	Poco efectivo (1)	Poco efectivo (2)	Poco efectivo (3)
		Débil (1)	Moderado (2)	Fuerte (3)

PÚBLICA

Tabla 61 Resultado de la valoración del control

Valoración del control	
Efectivo	9
Moderadamente efectivo	4 a 8
Poco efectivo	1 a 3

7.5.4. Valoración del riesgo posterior a la evaluación de los controles:

Para el cálculo de la probabilidad e impacto conforme a la ejecución de los controles se debe aplicar lo definido en la siguiente tabla, con esto se obtendrá la calificación del riesgo posterior a la implementación de estos, la cual será la que se tenga en cuenta para establecer el manejo:

Tabla 62 Criterios de Evaluación de los Controles para Disminuir Probabilidad e Impacto

Valoración del control o conjunto de controles.	Los controles ayudan a disminuir la probabilidad	Los controles ayudan a disminuir el impacto	# Columnas en la matriz de riesgo que se desplaza en el eje de la probabilidad	# Columnas en la matriz de riesgo que se desplaza en el eje de impacto
Efectivo	Directamente	Directamente	2	2
Efectivo	Directamente	Indirectamente	2	1
Efectivo	Directamente	No disminuye	2	0
Efectivo	No disminuye	Directamente	0	2
Moderadamente efectivo	Directamente	Directamente	1	1
Moderadamente efectivo	Directamente	Indirectamente	1	0
Moderadamente efectivo	Directamente	No disminuye	1	0
Moderadamente efectivo	No disminuye	Directamente	0	1

Fuente: Guía para la Administración de los Riesgos de Gestión Corrupción y Seguridad Digital y el Diseño de Controles en Entidades Públicas - DAFP.

7.6. Manejo del riesgo

Se puede aceptar el riesgo a decisión del dueño de los riesgos para aquellos que estén en nivel Bajo, que tengan identificados los controles existentes que se tienen implementados para que estén en ese nivel y que a su vez abarquen todas las causas.

Teniendo en cuenta el nivel inherente obtenido en la fase de valoración, 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

PUBLICA

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).

Si se comparte con otro proceso o regional, deberá contar con la aceptación del líder del proceso o director regional con el cual se quiere compartir, por lo cual deberán generar un memorando de aprobación en el cual ellos manifiesten de manera formal que están de acuerdo con que se comparta el riesgo, y remitir copia de este al gestor de Riesgos de Seguridad de la Información. Por otra parte, solo se puede transferir el riesgo si no es posible realizar el tratamiento porque este es del alcance de un tercero (pólizas de seguro, regionales, procesos).

Si se transfiere un riesgo a otro proceso o regional, deberá contar con la aceptación del nuevo dueño del riesgo, debiéndose generar un memorando de aprobación por parte del responsable y remitir copia de este al Gestor de Riesgos de Seguridad de la Información.

- Aceptar el riesgo: decisión que toma el dueño del riesgo de aceptar las consecuencias y probabilidad de un riesgo en particular, retener el riesgo mediante una decisión informada. Esta opción solo puede aplicarse para los riesgos que se encuentren en el nivel bajo que tengan identificados los controles existentes que se tienen implementados para que estén en ese nivel y que a su vez abarquen todas las causas (debe formalizarse esta decisión en el memorando relacionado en la condición general 7.2.3).

La priorización del riesgo se determina de acuerdo con el tiempo de atención que implicará el plan de tratamiento y los controles a implementar:

Tabla 63 Priorización del riesgo

ORDEN DE PRIORIDAD	TIEMPO DE ATENCIÓN	TIEMPO SUGERIDO DE TRATAMIENTO
1	Corto plazo	Hasta 4 meses
2	Mediano plazo	De 4 a 8 meses
3	Largo plazo	De 8 meses hasta cierre de la vigencia

De acuerdo con los resultados obtenidos en la fase de identificación, análisis y valoración de riesgos, se definen los controles a implementar, estableciendo adicionalmente una serie de actividades a realizar con el propósito de mitigar los riesgos identificados.

Las actividades para implementar serán aquellas que el dueño del riesgo defina para tratar los riesgos aceptados, y debe estar asociado a los controles establecidos en el anexo A de la norma ISO 27001

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

PÚBLICA

- 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.

7.7. 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, para determinar si son efectivos, moderadamente efectivos o poco efectivos, realizando los respectivos reportes al Gestor de Riesgos de Seguridad de la Información anexando las evidencias de cumplimiento, conforme a la programación que este último realice para la vigencia y realizando el análisis del comportamiento de cada control. El monitoreo se realizará a todos los riesgos identificados (bajo, moderado, alto y extremo) y en este se deberá indicar también si se ha materializado o no el riesgo.

7.8. Evaluación del riesgo residual:

Una vez finalizado los planes de tratamiento, se procede a realizar la evaluación del nivel residual, para esto nuevamente se determinará a partir de la aplicación de los controles y desarrollo de las actividades la probabilidad y el impacto con base a las tablas 44, 45 y 51. 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.

Para el cálculo de la probabilidad e impacto conforme a la ejecución de los controles se debe aplicar lo definido en los numerales 7.5.1, 7.5.2, 7.5.3 y 7.5.4.

Nivel Inherente VS Nivel Residual.

- Si el resultado de la evaluación del nivel residual es menor a la inherente, se concluyeque 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

PÚBLICA

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.

7.9. 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 implementar oportunidades de mejora. Por lo anterior, la oportunidad deberá entenderse como la consecuencia positiva frente al resultado del tratamiento del Riesgo, lo anterior quiere decir que puede identificarse una oportunidad de mejora conforme a las consecuencias positivas. Para esto, se debe registrar en la Suite Visión Empresarial (SVE) y remitirse un correo electrónico al Gestor de Riesgos de Seguridad de la Información informando el código de la oportunidad de mejora con la que quedó en el sistema.

7.10. Materialización

En el caso de materializarse un riesgo, este debe ser reportado de acuerdo con el procedimiento de gestión de incidentes de seguridad y privacidad de la información y ciberseguridad, en el sistema se deben identificar las actividades a seguir teniendo en cuenta los factores internos o externos que pueden propiciar el riesgo. Asimismo, se deberá analizar el riesgo, la efectividad de los controles actuales y validar en qué nivel queda posterior a la materialización, registrando los cambios respectivos en el sistema de información SVE; así mismo se deberá evaluar el plan de tratamiento. En caso de que el incidente de seguridad no cuente con un riesgo asociado se debe identificar y valorar el mismo de acuerdo con la metodología.

En caso de la materialización de un riesgo de tecnología emergente se utiliza la tipificación establecida y se deberá identificar

Los nuevos riesgos identificados deberán ser reportados 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.

8. ANEXOS

A1.G3.MI. Anexo Definiciones Guía de Gestión de Riesgos y Peligros del ICBF

9. FORMATOS

CODIGO	NOMBRE DEL FORMATO
F1.G3.MI	Formato Matriz de Riesgos Ambientales y del Sistema de Gestión Seguridad y Salud en el Trabajo
F2.G3.MI	Formato Matriz de Identificación de Peligros, Valoración de Riesgos y Determinación de los Controles.
F3.G3.MI	Formato Matriz de Riesgos Sistema de Gestión de Seguridad de la Información
F4.G3.MI	Formato Seguimiento Materialización De Riesgos Ambientales Y Ejecución De Controles

PÚBLICA

10. CONTROL DE CAMBIOS

Fecha	Versión	Descripción del Cambio
14/05/2024	V15	Se relacionan los cambios del documento por cada eje del SIGE: SGSI: El documento fue actualizado bajo la actualización de la ISO 27001:2022 Se actualizan los siguientes numerales del capítulo 7 GESTION DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION Y CONTINUIDAD LA OPERACIÓN: 7.2 Condiciones Generales, 7.6 Manejo del riesgo y 7.7 Monitoreo En el ítem 7 se actualiza el nombre como Gestión de Riesgos de Seguridad y Privacidad de la Información, Ciberseguridad y su generalidad Se actualiza el 7.1 Objetivos y el 7.2 Condiciones Generales se actualiza 7.2.1, 7.2.3,7.2.4,7.2.5,7.2.10, 7.2.12,7.2.13, 7.3.2 En el ítem 7.3.1 se actualiza el contexto y se agrega 7.3.1.1 Roles y Responsabilidades Se actualiza 7.3.4. Identificación de consecuencias positivas y negativas. Se actualiza la clasificación de los riesgos y se agrega Riesgos de Ciberseguridad En el ítem 7.10 se fortalece el tema de materialización SGA: Para la Gestión de Riesgos Ambientales se actualizó la metodología de acuerdo con lo establecido en la Guía para la Administración del Riesgo y el diseño de controles en entidades públicas Versión 6 y se incluye la política de operación No 20. SST: Capitulo Gestión de Peligros de Seguridad y Salud en el Trabajo: Se realiza revisión, actualización y se incluyen los términos y criterios en relación con la seguridad vial en concordancia con la Resolución 40595 del 2022 “Por la cual se adopta la metodología para el diseño, implementación y verificación de los Planes Estratégicos de Seguridad Vial y se dictan otras disposiciones” del Ministerio de Transporte. A nivel general se mejora el tamaño de las tablas y gráficas para facilitar su consulta y comprensión.
03/11/2023	V14	Capitulo Gestión de Peligros de Seguridad y Salud en el Trabajo: Se realiza revisión, actualización y se incluyen los términos y criterios en relación con la seguridad vial en concordancia con la Resolución 40595 del 2022 “Por la cual se adopta la metodología para el diseño, implementación y verificación de los Planes Estratégicos de Seguridad Vial y se dictan otras disposiciones” del Ministerio de Transporte. Capitulo Gestión de riesgos y oportunidades sistema de gestión de seguridad y salud en el trabajo – SGSST: Se realiza actualización de las políticas de operación en relación con los pasos e instrumentos del proceso de elaboración y aprobación de las matrices de riesgos del SGSST.
17/11/2022	V13	SGC: Se actualiza el capítulo de riesgos de calidad y corrupción incluyendo lo relacionado a la gestión de riesgos fiscales. SGSI: Se actualizan los siguientes numerales del capítulo 7 GESTION DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION, SEGURIDAD DIGITAL Y CONTINUIDAD DEL NEGOCIO: 7.2 Condiciones Generales, 7.6 Manejo del riesgo y 7.7 Monitoreo SST: Se actualizaron los siguientes numerales: 3.1. Objetivos, 3.2. Políticas operacionales para la identificación de peligros, valoración de riesgos y determinación de los controles de Seguridad y Salud en el Trabajo y 3.4. Metodología
14/10/2021	V12	SGSI: Se ajustan las fases del numeral 7 “Gestión de Riesgos de Seguridad y Privacidad de la Información Seguridad Digital y Continuidad del Negocio”, quedando de la siguiente manera: - 7.2. Condiciones Generales - 7.3. Identificación de riesgos de activos de información priorizados. - 7.4. Análisis del Riesgo. - 7.5. Valoración del riesgo. - 7.6. Manejo del Riesgo. - 7.7. Monitoreo. - 7.8. Evaluación Riesgo Residual. CALIDAD: Se especificó la estructura de identificaciones de los controles asociados a los riesgos de corrupción.

PÚBLICA

Fecha	Versión	Descripción del Cambio
		SST: Se realiza ajustes en el numeral 3 del presente guía denominado gestión de peligros de seguridad y salud en el trabajo, en el cual se modifica la introducción, objetivos, y el desarrollo de la metodología para la identificación de peligros, valoración de riesgo y determinación de peligros. Se realiza cambio del subtitulo entrada y condiciones generales por Políticas Operativas para la identificación de peligros, valoración de riesgos y determinación de los controles de Seguridad y Salud en el Trabajo, se modifican y adicionan criterios. Se actualizan e incluyen tablas de niveles de deficiencia para peligros provenientes de agentes higiénicos cualitativos y nota con referencia a valores cuantitativos peligros Higiénicos. Se actualizan tablas de determinación del nivel de exposición, probabilidad y nivel del riesgo, se modifica nota de riesgo no aceptable. Ajuste de los aspectos ambientales contenidos en el numeral 5 Gestión de riesgos de emergencia. Se actualiza el numeral 4 Gestión de Riesgos del Sistema de Gestión de Seguridad y Salud en el Trabajo-SGSST, incluyendo una política de operación y modificación del numeral 4.2.3 seguimiento y reporte. De otra parte, se actualiza la numeral gestión de riesgos de emergencia con el ajuste de objetivos, condiciones generales, identificación de amenazas, matriz de riesgos adicionando los valores 10%, 20%, 30%, modificación de elementos de Gestión en Seguridad y Salud y elementos ambientales.
27/11/2020	V11	Capítulo 2 Gestión de Riesgo de Calidad y Corrupción: Se eliminaron las políticas operaciones del capítulo teniendo en cuenta que se generó un procedimiento asociado a riesgos adicional se realizaron ajustes en cada una de las fases de la gestión de riesgos debido a la actualización de la guía de riesgos del DAFP del mes de diciembre de 2020. Capítulo 6 Gestión de Riesgos Ambientales: Se realizaron ajustes sobres las políticas operacionales del capítulo. Capítulo 7 Gestión de Riesgos SGSI:
23/04/2020	V10	En el capítulo de riesgos de calidad y corrupción se ajustaron las políticas operacionales, se ajustó la identificación de riesgos. Se agruparon varios capítulos en uno nuevo llamado generalidades. En el capítulo de los riesgos ambientales se realizaron los siguientes ajustes: inclusión de las indicaciones para el seguimiento al cumplimiento de los controles existentes y materialización de riesgos, consideración de las necesidades y expectativas de las partes interesadas en la identificación de los riesgos, inclusión del rol Coordinador Gestión del Soporte para las Regionales pequeñas. Ajustes en la definición de los criterios para determinar la solidez de los controles. Ampliación del concepto riesgos residual. Eliminación de la validación de la matriz de riesgos por parte de la Subdirección de Mejoramiento Organizacional para el nivel regional. Se elimina el anexo de la tabla número 23 Peligros y causas correspondiente al de Gestión de Peligros de Seguridad y Salud en el Trabajo, lo anterior dado a la necesidad de ajustar la matriz de identificación de peligros en cuanto a la evaluación de los peligros y valoración de los riesgos por parte de los referentes y profesionales a nivel país, adicional a esto se solicita la eliminación para que no se requiera una aprobación de la guía en caso que se cambien aspectos como la descripción o efectos posibles En el capítulo de riesgos de seguridad de la información se ajusta el numeral 7.2 condiciones generales, se ajusta una variable en la tabla de impacto y se actualiza imagen del numeral 7.6
12/11/2019	V9	Se elimina el anexo de la tabla numero 23 Peligros y causas correspondiente al capítulo 8 de Gestión de Peligros de Seguridad y Salud en el Trabajo, lo anterior dado a la necesidad de ajustar la matriz de identificación de peligros en cuanto a la evaluación de los peligros y valoración de los riesgos por parte de los referentes y profesionales a nivel país, adicional a esto se solicita la eliminación para que no se requiera una aprobación de la guía en caso que se cambien aspectos como la descripción o efectos posibles.
28/03/2019	V8	Se ajusto la guía de acuerdo con las necesidades de los cuatro ejes del Sistema Integrado de Gestión. Se ajustaron políticas operacionales del capítulo 7, se ajustaron los criterios de diseño de los controles, seguimiento a los controles, seguimiento a materialización. Se actualiza el capítulo de gestión de riesgos de seguridad y salud en el trabajo en el numeral Entradas y Condiciones Generales, incluyendo el ítem C, así como el capítulo de Gestión de riesgos de emergencia se incluye numeral 9 relacionado con riesgos y oportunidades para el Sistema de Gestión de la Seguridad y Salud en el Trabajo. Para el eje ambiental se explica la metodología de riesgos especificando las responsabilidades. Para el eje de Seguridad de la Información se modifica lo correspondiente a continuidad por el plan de continuidad de tecnología.
18/02/2019	V7	En el capítulo de gestión de riesgos de calidad y corrupción se ajustaron las políticas operacionales y el capítulo de evaluación de controles teniendo en cuenta el criterio de desviaciones de ejecución de control. Se ajusto todo el capítulo de gestión de riesgos en el eje de seguridad y salud en el trabajo debido a cambios normativos de los marcos de referencia. El capítulo del eje ambiental se cambió en su totalidad.

PÚBLICO

Fecha	Versión	Descripción del Cambio
		Se realizan ajustes a la metodología de gestión de riesgos de SGSI dando alcance a las adaptaciones realizadas en el marco de la implementación del MIPG en el año 2018 y la guía de gestión de riesgos del DAFP.
21/12/2018	V6	Se realizó ajustes de las políticas operacionales del capítulo de gestión de riesgos de calidad y corrupción Se actualizó links relacionados en varios capítulos de la guía. Se realizaron ajustes al capítulo de gestión de riesgos del eje ambiental teniendo en cuenta las observaciones enviadas vía correo electrónico por el eje, adicional se hicieron modificaciones solicitadas por la Oficina de Control Interno.
14/03/2018	V5	Se realizaron ajustes a la guía de gestión de riesgos de la entidad tomando como referencia la guía de gestión de riesgos del DAFP emitida en octubre del 2018. Se hicieron ajustes en los capítulos de calidad, y SST.
23/01/2018	V4	Se realizaron ajustes en los capítulos de seguridad de riesgos de emergencias, riesgos de calidad y corrupción. Se adiciono todo el capítulo de gestión de riesgos ambientales.
30/10/2017	V3	Se realizaron ajustes en los capítulos de Seguridad y Salud en el trabajo y en el capítulo de Seguridad de la Información y Continuidad del Negocio.
06/04/2017	V2	Se realizaron en el numeral 9 GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN, ajustes en los siguientes ítems: 9.0 Se determina que en la guía se incluye la gestión de Continuidad de Negocio 9.1 Se plantean nuevos objetivos. 9.2 se incluyen definiciones tomadas del DAFP – Tipos de riesgos 9.3 Continuidad de negocio forma parte como uno de los atributos afectados, para la identificación de riesgos. 9.5 se adicionó gráfica con el detalle de las fases que se ejecutan en la gestión de riesgos en el SGSI: análisis, tratamiento y resultados. Se actualiza la matriz de riesgos. Fase Análisis, se adiciona la casilla Tipo de riesgo. Fase Tratamiento: se reemplaza la casilla Acciones PHVA por Actividades y su seguimiento será cuatrimestral. 9.5.1 se actualizó el punto y, se eliminó el concepto de “Tomar o incrementar el riesgo” 9.5.2 se plantea una nueva tabla titulada Fuente Clasificación de Fuentes y causas de amenazas. 9.5.3 se suprime la tabla 10, debido a lo descrito anteriormente (9.5.2). 9.5.4 Se adicionó tabla de consecuencias positivas.
12/12/2016	V1	Con base en la Resolución 8080 de 11 de agosto de 2016 y la implementación del nuevo Modelo de operación por Procesos, se migra la Guía de Gestión de Riesgos del proceso de Mejora Continua al proceso de Mejora e Innovación. Se actualiza el Formato Matriz de Riesgos de Procesos (Calidad y Corrupción) incluyendo encabezado y pie de página. Se actualizaron los responsables del diligenciamiento de la Matriz de Identificación de Peligros, Valoración de Riesgos y Determinación de Controles y los anexos del Capítulo 7 “Gestión de Riesgos de Seguridad y Salud en el Trabajo”. Se actualiza el Formato Matriz de Identificación de Peligros, Valoración de Riesgos y Determinación de los Controles. Se actualizó el capítulo 8 "Gestión de Riesgo de Emergencia", según la metodología de análisis de riesgos con base a la Guía para elaborar planes de emergencias y contingencias del Fondo de Prevención y Atención de Emergencias – FOPAE, en conjunto con el listado de amenazas y las tablas de referencia de evaluación. Se actualizó el capítulo 9 “Gestión de Riesgos de Seguridad de la Información” debido a cambios en la herramienta para hacer el seguimiento, adicionalmente se amplía el concepto de oportunidad descrito en el numeral 9.5.5 Se actualiza el Formato Matriz Riesgos SGSI Se actualiza el formato de la Guía y se rotula como información pública.

PÚBLICA