DIRECCIÓN NACIONAL DE BOMBEROS DE COLOMBIA

PROCESO DE GESTIÓN DE ANÁLISIS Y MEJORA CONTINUA

MANUAL DE GESTIÓN DEL RIESGO

Introducción

La Dirección Nacional de Bomberos de Colombia - DNBC, reconociendo la importancia de implementar un sistema de gestión integral de riesgos que contribuya a la adecuada implementación de estrategias y procedimientos para el logro de sus objetivos, presenta la segunda versión del Manual de Gestión del Riesgos que adopta los lineamientos definidos por el Departamento Administrativo de la Función Pública – DAFP para las entidades del sector público en Colombia en su versión de diciembre de 2020, cuyos principales cambios están dados en la actualización y precisión de algunos elementos metodológicos para mejorar el ejercicio de identificación y valoración del riesgo, manteniendo la estructura general bajo tres pasos principales: política de administración de riesgos, identificación del riesgos y valoración del riesgo.

Este manual hace parte del Sistema de Gestión establecido por la DNBC, por cuanto, la Gestión del Riesgo contribuye al logro de los objetivos de la entidad a través de definición de lineamientos que permiten la articulación de los objetivos de la entidad, el desarrollo de la estrategia y la toma de decisiones de los procesos, así mismo está articulado con las políticas de transparencia, acceso a la información pública y lucha contra la corrupción liderada por la Secretaría de Transparencia y la de seguridad de la información en cabeza del Ministerio de Tecnologías de la Información y Comunicaciones (MinTIC) respectivamente.

El presente manual busca ser una herramienta sencilla, práctica y operativa, que permita a todos los funcionarios y contratista de la Dirección actúen participativamente en la Gestión del Riesgo de la entidad, de manera que se convierta en un elemento necesario en el desarrollo de sus actividades y se reconozca su importancia para el alcanzar sus objetivos, que de manera integral permitirá lograr la misión y visión de la DNBC.

Contenido

Índice de Tablas

Índice de Ilustraciones

1. OBJETIVO

Establecer las políticas y aspectos metodológicos con los cuales la Dirección Nacional Bomberos Colombia – DNBC identifica, analiza, valora y administra los riesgos institucionales, con el fin de alcanzar su misión, visión y objetivos estratégicos.

1.1. Objetivos Específicos

- ✓ Suministrar una metodología útil que permita a la DNBC gestionar de manera efectiva los riesgos que afectan el logro de los objetivos estratégicos y de proceso.
- ✓ Ofrecer herramientas de trabajo que permitan analizar, identificar, evaluar, tratar y monitorear los riesgos que deban ser gestionados por los responsables en la entidad (bajo el esquema de las líneas de defensa).
- ✓ Suministrar lineamientos que permitan a la alta dirección de la DNBC obtener un grado de confianza en el logro de sus objetivos, con base en una adecuada Gestión del Riesgo
- ✓ Unificar los aspectos comunes que existen con los riesgos de corrupción y riesgos de seguridad de la información, para facilitarle a la entidad la identificación de cada uno de estos riesgos, así como, el mejor tratamiento, fortaleciendo el enfoque preventivo.

2. ALCANCE

La política de Gestión del Riesgo, así como los lineamientos del presente manual son aplicables a todos los procesos de la entidad ejecutados por los funcionarios y contratistas en ejercicio de sus funciones y obligaciones a nivel nacional, con el fin de obtener un adecuado conocimiento y control de los riesgos en todos los niveles de la DNBC.

3. TÉRMINOS Y DEFINICIONES

Los conceptos que se mencionan a continuación son necesarios para una comprensión adecuada de la política y manual de riesgos.

- **Activo:** en el contexto de seguridad digital son elementos tales como aplicaciones de la organización, servicios web, redes, hardware, información física o digital, recurso humano, entre otros, que utiliza la organización para funcionar en el entorno digital.
- **Amenazas:** situación potencial de un incidente no deseado, el cual puede ocasionar daño a unsistema o a una organización.
- **Apetito de riesgo:** es el nivel de riesgo que la entidad puede aceptar en relación con sus objetivos, el marco legal y las disposiciones de la alta dirección. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.
- **Capacidad del riesgo:** es el máximo valor del nivel de riesgo que una entidad puede soportar y a partir del cual se considera por la alta dirección y el órgano de gobierno que no sería posible el logro de los objetivos de la entidad.
- **Causa:** todos aquellos factores internos y externos que solos o en combinación con otros,

pueden producir la materialización de un riesgo.

- **Causa inmediata:** circunstancias bajo las cuales se presenta el riesgo, pero no se constituye la causa principal o base para que se presente el riesgo.
- **Causa raíz:** causa principal o básica, corresponde a las razones por la cuales se puede presentar el riesgo.
- **Confidencialidad:** propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados.
- **Consecuencia:** los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas.
- **Control:** medida que permite reducir o mitigar un riesgo, estas medidas pueden definirse en políticas, procesos, herramientas de apoyo, prácticas u otras acciones.
- **Disponibilidad:** propiedad de ser accesible y utilizable a demanda por una entidad.
- **Entorno digital**: Ambiente, tanto físico como virtual, sobre el cual se soporta la economía digital. Siendo esta última la economía basada en tecnologías, cuyo desarrollo y despliegue se produce en un ecosistema caracterizado por la creciente y acelerada convergencia entre diversas tecnologías, que se concreta en redes de comunicación, equipos de hardware, servicios de procesamiento y tecnologías web. (CONPES 3854, pág. 87).
- **Entorno digital abierto**: En el que no se restringe el flujo de tecnologías, de comunicaciones o de información, y en el que se asegura la provisión de los servicios esenciales para los ciudadanos y para operar la infraestructura crítica. (CONPES 3854, pág. 87).
- **Evento de seguridad de la información:** Ocurrencia que indica una posible brecha de seguridad de la información o falla de los controles. (ISO/IEC 27035:2016).
- **Factores de riesgo:** son las fuentes generadoras de riesgos.
- **Gestión del Riesgo:** proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos.
- **Impacto:** se entiende como las consecuencias que puede ocasionar a la organización la materialización del riesgo.
- **Integridad:** es propiedad de exactitud y completitud que posee la información.
- **Incidente digital:** Evento intencionado o no intencionado que puede cambiar el curso esperado de una actividad en el medio digital y que genera impactos sobre los objetivos. (CONPES 3854, pág. 87).
- **Incidente de seguridad de la información:** Uno o múltiples eventos de seguridad de la información relacionados e identificados que pueden dañar los activos de información de la organización o comprometer sus operaciones. (ISO/IEC 27035:2016).
- **Mapa de riesgos:** documento que contiene la información resultante de la identificación, análisis, evaluación y tratamiento de los riesgos de la entidad.
- **Nivel de riesgos:** es el valor que se determina a partir de combinar la probabilidad de ocurrencia de un evento potencialmente dañino y la magnitud del impacto que este evento traería sobre la capacidad institucional de alcanzar los objetivos. En general la fórmula de nivel de riesgos es, probabilidad x impacto, sin embargo, puede relacionarse las

variables a través otras maneras diferentes a la multiplicación, por ejemplo, mediante una matriz de probabilidad e impacto.

- **Plan Anticorrupción y de Atención al Ciudadano:** plan que contempla la estrategia de lucha contra la corrupción y que debe ser implementada por todas las entidades del orden nacional, departamental y municipal.
- **Probabilidad:** se entiende como la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o la actividad que se esté analizando. La probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de un año.
- **Riesgo:** para efectos de este manual se entiende como riesgo el efecto que se causa sobre los objetivos de las entidades debido a eventos potenciales. Los eventos potenciales hacen referencia a la posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por ocurrencia de acontecimientos externos. Nota: La NTC-GTC137define el riesgo como: posibilidad que suceda algún evento que tendrá un impacto sobre el cumplimiento de los objetivos. Se expresa en términos de probabilidad y consecuencias.
- **Riesgo de corrupción:** posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.
- **Riesgo residual:** es el resultado de aplicar la efectividad de los controles al riesgo inherente.
- **Riesgo de seguridad de la información:** posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño de un activo de la información. Suele considerarse como una combinación de la posibilidad de un evento y sus consecuencias. (ISO/IEC 27000).
- **Tolerancia del riesgo:** es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del apetito del riesgo determinado por la entidad.
- **Vulnerabilidad:** representa la debilidad de un acto o de un control que puede ser explotada por una amenaza.

4. NORMATIVIDAD

- Ley 489 de 1998 "Por la cual se dictan normas sobre la organización y funcionamiento de las entidades del orden nacional, se expiden las disposiciones, principios y reglas generales para el ejercicio de las atribuciones previstas en los numerales 15 y 16 del artículo 189 de la Constitución Política y se dictan otras disposiciones."
- Ley 872 de 2003 "Por la cual se crea el sistema de gestión de la calidad en la Rama Ejecutiva del Poder Público y en otras entidades prestadoras de servicios".
- Ley 1474 de 2011 "Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública."
- Ley 2195 de 2022 "Por medio de la cual se adoptan medidas en materia de transparencia, prevención y lucha contra la corrupción y se dictan otras disposiciones"
- Decreto 1083 de 2015 "Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública"

- Decreto 1499 DE 2017 "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"
- Decreto 648 de 2017 "Por el cual se modifica y adiciona el Decreto 1083 de 2015, Reglamentario Único del Sector de la Función Pública"
- Decreto 1008 de 2018 "Por medio del cual se expide el Decreto Reglamentario Único del Sector Presidencia de la República" que en el Titulo 4 se establece el "Plan Anticorrupción y de Atención al Ciudadano"
- Resolución 00500 de 2021 del Ministerio de Tecnologías de la Información y las Comunicaciones "Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital"
- Resolución 587 de 2021 de la Dirección Nacional de Bomberos de Colombia "Por medio de la cual se actualiza las disposiciones que reglamentan el Sistema de Gestión, se conforman los equipos de trabajo y líneas de defensa institucional, en el marco de referencia del Modelo Integrado de Planeación y Gestión de la Dirección Nacional de Bomberos de Colombia"
- Directiva presidencial 09 de 1999 "Lineamientos para la implementación de la política de lucha contra la corrupción"
- NTC GTC 137:2011 "Norma Técnica Colombiana Gestión del Riesgos. Vocabulario"
- NTC ISO 9001: 2015 "Norma Técnica Colombiana del Sistema de Gestión de Calidad"
- NTC ISO 31000:2018 "Norma Técnica Colombiana del Sistema de Gestión del Riesgos"
- Guía "Estrategias para la Construcción del Plan Anticorrupción y de Atención al Ciudadano" de la Secretaría de Transparencia de la Presidencia de la República versión 2 de 2015
- Guía para la administración del riesgo y el diseño de controles en entidades públicas. Riesgos de Gestión, Corrupción y Seguridad Digital. Versión 4 octubre de 2018.
- Guía de orientación de aplicación del Modelo Nacional de Gestión de Riesgos de Seguridad Digital - GRSD en el sector público, territoriales y gobierno nacional. 2018
- Guía para la administración del riesgo y el diseño de controles en entidades públicas. Versión 5 de diciembre de 2020.
- Manual operativo Sistema de Gestión MIPG. Versión 4 de mayo de 2021.
- CONPES 3854 Política Nacional de Seguridad Digital. Marzo 2016,
- CONPES 3995 de 2020, Política Nacional de Confianza y Seguridad Digital. Julio 2020
- ISO/IEC 27001:2013 Estándar internacional para la Seguridad de la Información en las organizaciones.

5. POLÍTICA INTEGRAL DE RIESGOS

La Dirección Nacional de Bomberos de Colombia – DNBC como líder en la implementación de la Gestión del Riesgos contra incendios, los preparativos y atención de rescates en todas sus modalidades y la atención de incidentes con materiales peligrosos, define la presente política integral de riesgos basada en los lineamientos impartidos por el Departamento Administrativo de la Función Pública - DAFP y la normatividad vigente aplicable, manifiesta su compromiso con la Gestión del Riesgos para analizar, identificar, evaluar, tratar y monitorear y de forma sistemática, todas aquellas amenazas que signifiquen un riesgo para lograr los objetivos institucionales.

La Alta Dirección y el Comité Institucional de Coordinación de Control Interno, como líderes de la Gestión del Riesgo de la entidad, se comprometen con su desarrollo y mantenimiento eficaz, aportando los recursos necesarios que permitan su adecuado funcionamiento y mejoramiento continuo de manera transversal en todos los procesos.

Se considerarán como elementos fundamentales de la Gestión del Riesgo, los siguientes:

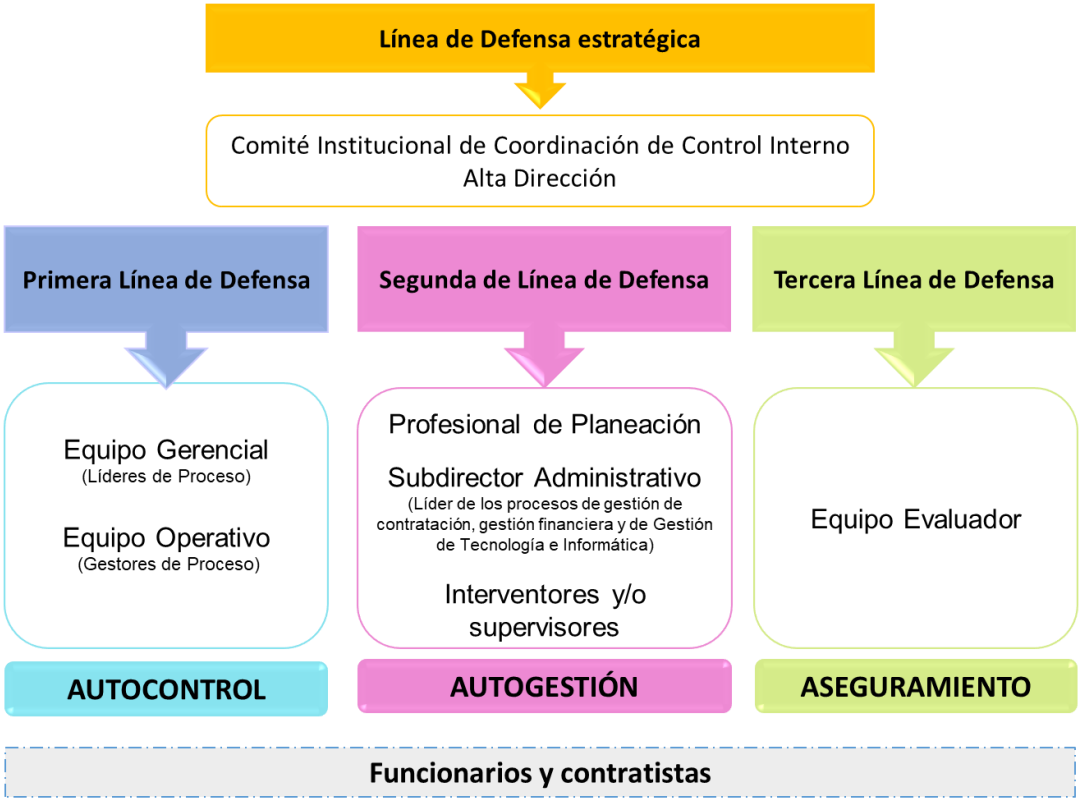
- Motivación y compromiso en identificar debilidades e implementar mejoras basados en un enfoque de procesos.
- Recurso humano capacitado e informado, a través de habilidades, perfiles y entrenamiento necesario.
- Articulación de la misión, visión y objetivos estratégicos con los objetivos de los procesos de la entidad.
- Integridad y consistencia de los procesos estratégicos, misionales, de apoyo y, de evaluación y control.
- Pertinencia y oportunidad en el reporte de la información generada por los procesos para la gestión del riesgo.
- Autocontrol y autogestión que se beben ejercer en las actividades de la DNBC, de acuerdo con la estructura, roles y responsabilidades que al interior de los procesos existan.
- Transparencia en la información de riesgos identificados, tratados y las decisiones institucionales ejecutadas.
- Fortalecimiento en el enfoque estratégico en todos aquellos asuntos importantes para la entidad. En este contexto, y a fin de mejorar continuamente, la Gestión del Riesgo estará orientada analizar, identificar, evaluar, tratar y monitorear los riesgos potenciales asociados a los procesos misionales, estratégicos y de apoyo, que puedan afectar la misión y objetivos de la DNBC.

Para el cumplimiento de lo anterior, la DNBC revisará al menos una vez al año el Manual de Gestión del Riesgos, que incluye la política y metodología.

5.1. Responsabilidades de la Gestión del Riesgo

La Dirección Nacional de Bomberos de Colombia opera mediante la estructura de líneas de defensa, así:

Ilustración 1: Líneas de Defensa de la DNBC



Fuente: Líneas de defensa de la DNBC

Cada línea de defensa tiene un rol frente a la Gestión del Riesgo, la cual se describe a continuación:

5.1.1. Línea Estratégica

Es la instancia decisoria dentro del Sistema de Control Interno, está bajo la responsabilidad de la Alta Dirección y del Comité Institucional de Coordinación de Control Interno; su rol principal es analizar los riesgos y amenazas institucionales, que puedan afectar el cumplimiento de los planes estratégicos, así como definir el marco general para la Gestión del Riesgo (política y metodología) y el cumplimiento de los planes de la entidad, sus roles y responsabilidades frente a la Gestión del Riesgo son:

Comité Institucional de Coordinación de Control Interno

a. Someter a aprobación del representante legal la política de administración del riesgo y hacer seguimiento, en especial a la prevención y detección de fraude y mala conducta.

b. Aprobar la política Gestión del Riesgo y evaluar su cumplimiento.

c. Determinar los niveles de tolerancia y aceptación del riesgo.

d. Revisar y pronunciarse sobre el informe de Gestión del Riesgo anual sobre los resultados del sistema.

e. Evaluar las medidas de control para los riesgos en niveles alto y extremo y, tomar las acciones necesarias para su tratamiento en el caso que los controles no sean efectivos para su reducción.

f. Monitorear de manera permanente los riesgos de corrupción.

g. Revisar y aprobar los informes cuatrimestrales de Gestión del Riesgo de corrupción.

h. Monitorear el estado de los riesgos aceptados (apetito por el riesgo), con el fin de identificar cambios sustantivos que afecten el funcionamiento de la entidad, mediante el informe semestral emitido por el responsable de la segunda línea de defensa

i. Verificar los riesgos relacionados con el manejo de información clasificada o reservada.

Representante de la Alta Dirección

a. Proveer los recursos necesarios para implementar y mantener en funcionamiento, de forma efectiva y eficiente de la Gestión del Riesgo.

b. Asegurar que establezcan, socialicen y mantengan los procesos necesarios para la implementación, mejoramiento y sostenibilidad de la Gestión del Riesgo de la DNBC.

5.1.2. Primera Línea de Defensa

Esta línea está bajo la responsabilidad del equipo gerencial y el equipo operativo; su rol principal es el mantenimiento efectivo de controles internos y la ejecución de gestión de riesgos y controles en el día a día. Para ello, orienta el desarrollo e implementación de políticas y procedimientos internos, asegurando que sean compatibles con las metas y objetivos de la entidad y emprende acciones de mejoramiento para su logro, a través del **"Autocontrol"**.

Equipo Gerencial o Líderes de Proceso

a. Identificar y valorar los riesgos que pueden afectar el logro de los objetivos institucionales, así como, definir y diseñar los controles a dichos riesgos, evitando la materialización de riesgos.

b. Establecer las responsabilidades a partir de la política de administración del riesgo, para controlar los riesgos específicos bajo la supervisión de la alta dirección. Con base en esto, establecer los mapas de riesgos.

c. Mantener controles internos efectivos, para ejecutar procedimientos de riesgo y control, en el día a día.

d. Efectuar seguimiento a los riesgos y controles de su proceso.

e. Analizar el contexto de los procesos del cual es líder, en conjunto con sus equipos de trabajo, que permita realizar una adecuada identificación de los riesgos.

f. Formular los planes de acción y hacer seguimiento de su implementación y efectividad para tratar los riesgos.

g. Reportar los eventos, acciones o fallas que conlleven a la posible materialización de riesgos de sus procesos o de otros procesos.

h. Construir y enviar al responsable del proceso de Gestión de Análisis y Mejora Continua o quien haga sus veces, el informe de monitoreo de riesgo de gestión y corrupción en las fechas definidas por la segunda línea de defensa.

i. Actualizar el mapa de riesgos en caso de ser necesario y hacer seguimiento al cumplimiento de las acciones dispuestas.

j. Reportar y facilitar las evidencias que se requieran en el seguimiento de los riesgos que realiza el proceso de Evaluación y Seguimiento, de acuerdo con el mecanismo dispuesto por la DNBC.

k. Participar en los procesos de aprendizaje que se programen y facilitar la asistencia de los funcionarios y contratistas de su equipo de trabajo.

l. Coordinar con sus equipos de trabajo, a fin de contar con información clave para el seguimiento o autoevaluación de sus procesos y reportar a la segunda línea de defensa sus resultados.

m. Proponer cuando lo considere necesario las mejoras a la Gestión del Riesgo de la DNBC.

Gestores de Proceso

Conformado por los representantes de los procesos de la DNBC, su función principal frente a la Gestión del Riesgos es apoyar a los líderes de proceso, en el ejercicio de la administración de riesgos, informando sobre la incidencia de los mismos en el logro de objetivos, evaluando si la valoración del riesgo es la apropiada, asegurando que se identifiquen riesgos de gestión y corrupción, efectuando seguimientos a las acciones y controles establecidos en los mapas de riesgos, conforme a la política de administración de riesgo establecida por la entidad. Para tal fin los gestores de proceso deben:

a. Apoyar al equipo gerencial, en el ejercicio de la administración de riesgos, informando sobre la incidencia de estos en el logro de objetivos, evaluando si la valoración del riesgo es la apropiada, asegurando que se identifiquen riesgos de fraude, efectuando seguimientos a las acciones y controles establecidos en los mapas de riesgo, conforme a la política de administración de riesgo establecida para la DNBC.

b. Apoyar al Equipo Gerencial en la construcción de los informes de monitoreo de los riesgos que se reporta al proceso de Gestión de Análisis y Mejora Continua.

c. Presentar propuestas de mejora relacionadas con la administración de los riesgos al líder del proceso para su análisis y evaluación

d. Monitorear y registrar los cambios que se presenten en los riesgos de tipo legal, regulatorio y de cumplimiento y actualizar el Normograma respectivo.

e. Apoyar al Equipo Gerencial en el monitoreo permanente de los cambios en el entorno (interno y externo) que puedan afectar la efectividad del SCI.

f. Participar activamente en el proceso de diseño, desarrollo, implementación, mantenimiento, difusión y mejora de los riesgos, controles y planes de acción definidos en

el mapa de riesgos de su proceso.

g. Hacer seguimiento a los planes de acción definidos para atender el tratamiento de los riesgos, reportar al líder del proceso cualquier situación que afecte el cumplimiento oportuno de los planes de acción definidos y proponer alternativas para subsanar dichas situaciones.

h. Realizar de manera permanente el seguimiento de los controles y planes de acción definidos en las matrices de riesgos de sus procesos y reportar al proceso de Gestión de Análisis y Mejora Continua cualquier evento que genere un cambio en los riesgos, controles, valoración o en los planes de acción.

i. Fomentar la cultura de la Gestión del Riesgos, reconociendo su importancia para el logro de los objetivos del proceso que impactan los objetivos estratégicos de la DNBC.

j. Reportar los eventos, acciones o fallas que conlleven a la posible materialización de riesgos de su proceso o de otros procesos.

k. Participar en las reuniones, capacitaciones, y talleres que sean programados, relacionados para el diseño, desarrollo, implementación, mantenimiento, difusión y monitoreo de la Gestión del Riesgos.

5.1.3. Segunda Línea de Defensa

Conformada por el profesional con funciones de Planeación o quien haga sus veces, el subdirector Administrativo como responsable de los procesos de: gestión contractual, gestión financiera y gestión de Tecnología e Informática y los supervisores e interventores de los contratos suscritos por la DNBC. Su rol principal es asegurar que los controles y procesos de gestión del riesgo de la 1ª Línea de Defensa estén diseñados apropiadamente y funcionen como se pretende; así mismo, consolidar y analizar la información sobre temas clave para la entidad, base para la toma de decisiones necesarias para evitar materializaciones de riesgos, todo lo anterior enmarcado en la **"autogestión".**

Profesional con funciones de Planeación o quien haga sus veces

El profesional con funciones de Planeación o quien haga sus veces junto con su equipo de trabajo es responsable de:

a. Realizar aseguramiento de que los controles y procesos de gestión del riesgo de la primera línea de defensa sean apropiados y funcionen correctamente.

b. Supervisar la implementación de prácticas de gestión de riesgo eficaces, mediante:

- Coordinar y verificar de la construcción y/o actualización de los riesgos de corrupción, gestión y seguridad de la información.
- Realizar seguimiento de la implementación de los procesos y procedimientos definidos para la gestión del riesgo en la DNBC.
- Revisar por lo menos una vez al año la política y manual de la Gestión del Riesgo definido en la DNBC y proponer los cambios necesarios para su actualización.
- Acompañar, orientar y entrenar a los líderes y gestores de proceso en la analizar, identificación, evaluación y tratamiento del riesgo.

- Verificar de la ejecución de los reportes de evaluaciones de autocontrol, por parte de la primera línea de defensa, monitoreando sus riesgos.
- Consolidar el mapa de riesgos, a partir de la información construida por los líderes de los procesos y su equipo de trabajo.
- Cuando lo considere necesario, presentar las propuestas de mejora necesarias para fortalecer la Gestión del Riesgos de la DNBC.
- Informar al representante de la Alta Dirección sobre las necesidades de capacitación de la Gestión del Riesgos de la DNBC.
- Mantener un canal de comunicación abierto con los procesos facilitando la aclaración de términos o técnicas para el proceso de levantamiento de mapas de riesgos en cada una de sus etapas, incluyendo los riesgos de corrupción.
- Analizar los reportes de eventos presentados por la primera línea de defensa para identificar riesgos materializados, reportar su incidencia y solicitar al proceso correspondiente las acciones correctivas necesarias.

c. Generar reportes periódicos al Comité Institucional de Coordinación de Control Interno acerca del cumplimiento de las metas y los objetivos en relación con la gestión integral del riesgo.

d. Comunicar al Comité Institucional de Coordinación de Control Interno, como resultado de la evaluación de la gestión del Riesgo, las deficiencias para tomar las medidas correctivas, según corresponda.

e. Realizar monitoreo permanentemente los cambios en el entorno (interno y externo) que puedan afectar la efectividad del Sistema de Control Interno.

f. Revisar las exposiciones al riesgo con los grupos de valor, proveedores, sectores económicos u otros (monitoreo del contexto estratégico).

g. Verificación, en el marco de la política de riesgos institucional, que la identificación y valoración del riesgo de la primera línea sea adecuada frente al logro de objetivos y metas.

h. Verificar de la adecuada identificación de los riesgos relacionados con fraude y corrupción.

i. Verificar que el diseño del control establecido por la primera línea de defensa sea pertinente frente a los riesgos identificados, analizando: los responsables y su adecuada segregación de funciones, propósito, periodicidad, tratamiento en caso de desviaciones, forma de ejecutar el control y evidencias de su ejecución, y efectuar las recomendaciones a que haya lugar ante las instancias correspondientes (primera, segunda, y línea estratégica).

j. Monitorear los riesgos acordes con la política de administración de riesgos establecida.

k. Solicitar los recursos necesarios para implementar y mantener en funcionamiento, de forma efectiva y eficiente la Gestión de Riesgos de la DNBC.

l. Presentar una vez al año un informe general sobre el resultado de la evaluación realizada por la segunda línea de defensa de la Gestión del Riesgo de la DNBC, informando sobre los aspectos claves de su implementación y estado actual de los riesgos de la entidad (Exposición al riesgo acorde con la política institucional, el cumplimiento legal y regulatorio,

el logro de los objetivos estratégicos o institucionales y la confiabilidad de la información financiera y no financiera).

m. Trabajar de forma coordinada con el proceso de Evaluación y Seguimiento, con el fin de velar por la difusión de la política y la metodología de Gestión del Riesgo en toda la entidad.

Subdirector Administrativo

Como responsable de los procesos de gestión contractual, gestión financiera, gestión de tecnología e informática, así como del Sistema de Seguridad y Salud en el Trabajo (SG-SST), frente a las metodologías propias que definan estos procesos y el SG-SST, debe:

a. Coordinar la construcción y/o actualización de las metodologías para propias de gestión contractual, gestión financiera, gestión de tecnología e informática y el SG-SST para la gestión del riesgo.

b. Verificar la adecuada implementación de las metodologías propias de los procesos gestión contractual, gestión financiera, gestión de tecnología e informática y el SG-SST

c. Supervisar la eficacia e implementación de las prácticas de gestión de riesgo realizadas por la primera línea de defensa, correspondientes a las metodologías propias de los procesos gestión contractual, gestión financiera, gestión de tecnología e informática y el SG-SST.

Supervisores y/o interventores de contratos

Son los responsables asignados por la DNBC para actuar como supervisores y/o interventores de los contratos vigentes en la entidad, frente a la Gestión del Riesgo su responsabilidad es:

a. Hacer seguimiento a las obligaciones definidas en el objeto contractual

b. Hacer seguimiento a los acuerdos de niveles servicios definidos

c. Verificar la vigencia de las garantías definidas en el contrato (pólizas)

d. Reportar los eventos, acciones o fallas que conlleven a la posible materialización de riesgo.

5.1.4 Tercera Línea de Defensa

Esta línea está bajo la responsabilidad del asesor de control interno, líder del proceso de Evaluación y Seguimiento. Su rol principal es proporcionar aseguramiento basado en el más alto nivel de independencia y objetividad sobre la efectividad del Sistema de Control Interno, a través de la auditoría interna que cubre todos los componentes de Sistema. Frente a la Gestión del Riesgo es responsable de:

a. Orientar técnicamente y recomendar frente a la administración del riesgo en coordinación con el Profesional Especializado con funciones de Planeación o quien haga sus veces, con el fin de garantizar el cumplimento efectivo de los objetivos.

b. Monitorear la exposición de la organización al riesgo y realizar recomendaciones con alcance preventivo.

c. Asesorar proactiva y estratégicamente a la Alta Dirección, Equipo Gerencial y Equipo Operativo, en materia de control interno y sobre las responsabilidades en materia de riesgos.

d. Informar a la alta dirección y a todos los niveles de la entidad sobre las responsabilidades en materia de riesgos.

e. Asesorar en coordinación con la segunda línea de defensa en metodologías para la identificación y administración de riesgos.

f. Realizar el seguimiento al mapa de riesgos institucional de la Dirección Nacional de Bomberos de Colombia.

g. Revisar la efectividad y la aplicación de los controles, planes de contingencia y actividades de monitoreo vinculadas a riesgos claves de la entidad.

h. Alertar sobre la probabilidad de riesgo de fraude o corrupción en las áreas auditadas.

i. Recomendar mejoras a la política de Gestión del Riesgo.

j. Evaluar la efectividad de las acciones desarrolladas por la segunda línea de defensa en aspectos como: cobertura de riesgos, cumplimientos de la planificación, mecanismos y herramientas aplicadas, entre otros, y generar observaciones y recomendaciones para la mejora.

k. Comunicar el resultado de la evaluación de la gestión del Riesgo a la alta dirección o a las partes responsables para tomar las medidas correctivas.

5.1.5. Funcionarios y Contratistas

En general todos los funcionarios y contratistas de la Dirección Nacional de Bomberos de Colombia deben atender las disposiciones establecidas para el adecuado funcionamiento de la Gestión del Riesgo y son responsables de:

a. Conocer y apropiar de las políticas, procedimientos, manuales, instructivo y otras herramientas diseñadas por la entidad frente a la Gestión del Riesgo que permitan tomar acciones para el autocontrol en sus puestos de trabajo.

b. Apoyar en la implementación de los planes de acción definidos para atender el tratamiento de los riesgos.

c. Ejecutar los controles definidos en los procesos para mitigar los riesgos.

d. Identificar e informar al líder de proceso las situaciones que podrían generar un acto de corrupción en los procesos de la DNBC.

e. Cumplir la ley y denunciar actos y personas que contravengan la legalidad.

f. Reportar los eventos, acciones o fallas que conlleven a la posible materialización de riesgos de su proceso o de otros procesos.

g. Participar en los procesos de aprendizaje programados.

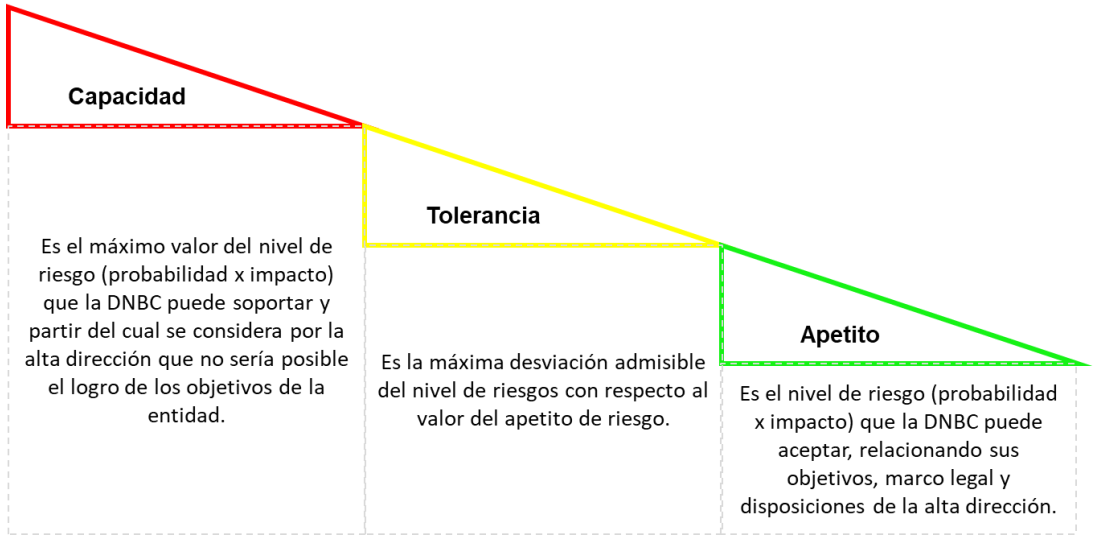
5.1.6. Comité de Gestión y Desempeño (Comité Directivo)

Analizar la gestión del riesgo de la DNBC, así como la aplicación de las mejoras.

5.2. Definición del apetito del riesgo en la DNBC

Con el fin de determinar el nivel de riesgo, se analiza la capacidad, apetito y tolerancia al riesgo, que de acuerdo con la misión, visión y plan estratégico de la DNBC puede aceptar para alcanzar sus objetivos, determinado de esta manera las escalas de impacto y probabilidad que en conjunto miden el nivel de los riesgos identificados y que permitirán a la entidad tomar decisiones para su tratamiento.

Ilustración 2: Marco para determinar el apetito del riesgo



Fuente: Gráfica adaptada del Manual Operativo MIPG

Una vez analizados los conceptos, la Dirección Nacional de Bomberos de Colombia determina de conformidad a las tablas de probabilidad e impacto, los niveles de riesgos que son aceptados y tolerados por la entidad, así:

- Riesgos de gestión y de seguridad de la información: se aceptan los riesgos de calificación "baja" y "moderada", para los riesgos de calificación "alta" y "extrema" se deben tomar medidas de tratamiento para su gestión.
- Riesgos de corrupción: no hay aceptación del riesgo, es decir que estos riesgos deben tener actividades de reducción o eliminación.

El detalle de las medidas de tratamiento se describe en el numeral 5.5. Tratamiento del Riesgo del presente manual.

5.3. Niveles para calificar la probabilidad

La probabilidad es una medida que determina el número de veces que puede ocurrir un riesgo. Para efectos de esta metodología, el análisis de la probabilidad de ocurrencia estará asociada a la **exposición del riesgo,** es decir las veces en las cuales se realiza una actividad susceptible a la materialización del riesgo en el periodo de un año. La siguiente tabla presenta los niveles de medición de las frecuencias de las actividades con las cuales serán valorados los riesgos identificados.

Tabla 1: Criterios para definir el nivel de probabilidad

	Frecuencia de la Actividad	Probabilidad
Muy Baja	La actividad conlleva el riesgo se ejecuta como máximo 2 veces por año.	20%
Baja	La actividad conlleva el riesgo se ejecuta de 3 a 24 veces por año.	40%
Media	La actividad conlleva el riesgo se ejecuta de 25 a 60 veces por año	60%
Alta	La actividad conlleva el riesgo se ejecuta de 61 a 360 veces por año	80%
Muy Alta	La actividad conlleva el riesgo se ejecuta más de 360 veces por año	100%

Fuente: Adaptación propia

5.4. Niveles para calificar el impacto

El impacto es la magnitud del riesgo materializado, en otras palabras, es la medición del efecto que puede acarrear sobre la entidad, medido en relación con la afectación económica y/o reputacional que le puede generar.

Al igual que en la probabilidad el impacto se medirá en relación con la **exposición del riesgo,** es decir que, en el caso de la afectación económica se evaluará el valor promedio asociado a la actividad susceptible de materialización de un riesgo. En relación con la afectación reputacional esta corresponde al deterioro que puede tener la imagen de la entidad debido entre otras a fallas de la información o en la prestación en el servicio.

Tabla 2: Criterios para definir el nivel de impacto

	Afectación Económica (al presupuesto de la DNBC)	Afectación a la Reputación (buen nombre de la DNBC)	Impacto
Leve	Afectación al presupuesto menor a 10 SMLMV	El riesgo afecta la imagen de algún proceso de la DNBC a nivel interno y es de conocimiento del líder del proceso.	20%
Menor	Afectación al presupuesto entre 10 y 50 SMLMV	El riesgo afecta la imagen de la DNBC a nivel interno y es de conocimiento de la Dirección General y el Comité de Coordinación de Control Interno.	40%
Moderado	Afectación al presupuesto entre 50 y 100 SMLMV	El riesgo afecta la imagen de la DNBC frente a sus proveedores y Cuerpos de Bomberos, con relevancia en el logro de los objetivos de la institución.	60%
Mayor	Afectación al presupuesto entre 100 y 500 SMLMV	El riesgo afecta la imagen de la DNBC ante alguna de las siguientes partes: organismos del orden nacional, entes de control, alguna comunidad, alcaldía, gobernación, delegación o coordinación de bomberos o Junta Nacional de Bomberos.	80%
Catastrófico	Afectación al presupuesto mayor a 500 SMLMV	El riesgo afecta la imagen de la DNBC a nivel nacional, con efecto publicitario sostenido a nivel país.	100%

Fuente: Adaptación propia

En el formato del mapa de riesgos de la DNBC, en su valoración de impactos reputacionales se relaciona la lista de las partes interesadas de acuerdo con la tabla de valoración (tabla No. 2), con el fin que el proceso identifique cuál de estas partes interesadas puede verse afectada frente a un impacto reputacional, es de anotar que siempre se debe escoger el escenario más crítico para que la evaluación se adecuada.

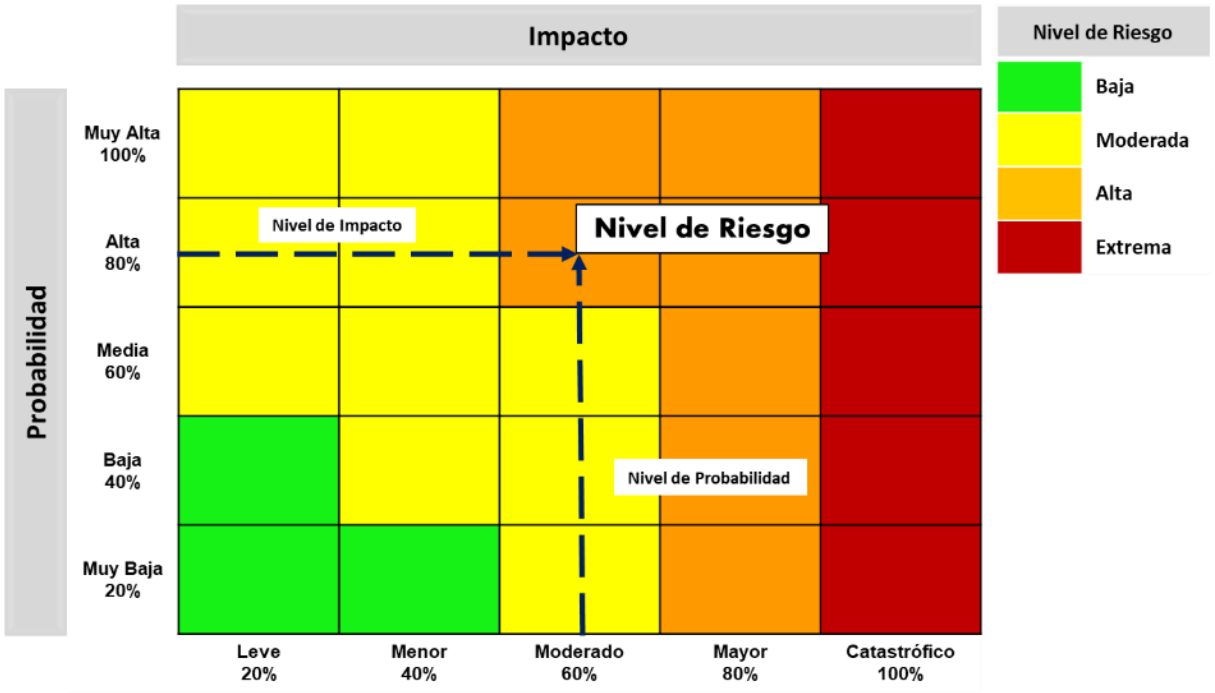
En el mapa de riesgos se listará de la siguiente manera

- Un proceso: Corresponde a la afectación reputacional de nivel de impacto leve descrito en la tabla.
- Más de un proceso y el CICCI: Corresponde a la afectación reputacional de nivel de impacto menor descrito en la tabla.
- Proveedores y Cuerpos de Bomberos: Corresponde a la afectación reputacional de nivel de impacto moderado descrito en la tabla.
- O.Nacional - E.Control – comunidad – alcaldía – gobernación - D/C Bomberos - JNB: Corresponde a la afectación reputacional de nivel de impacto mayor descrito en la tabla.
- A nivel nacional: Corresponde a la afectación reputacional de nivel de impacto catastrófico descrito en la tabla.

  Nota: Para la valoración del impacto de los riesgos de corrupción se utilizarán tablas independientes que se presentan describen en el capítulo 6 Desarrollo de la Gestión del Riesgos de la DNBC.

El resultado del cruzar la probabilidad y el impacto se denominará Nivel de Riesgos.

Ilustración 3: Demostración del Nivel de Riesgo



Fuente: Adaptación propia

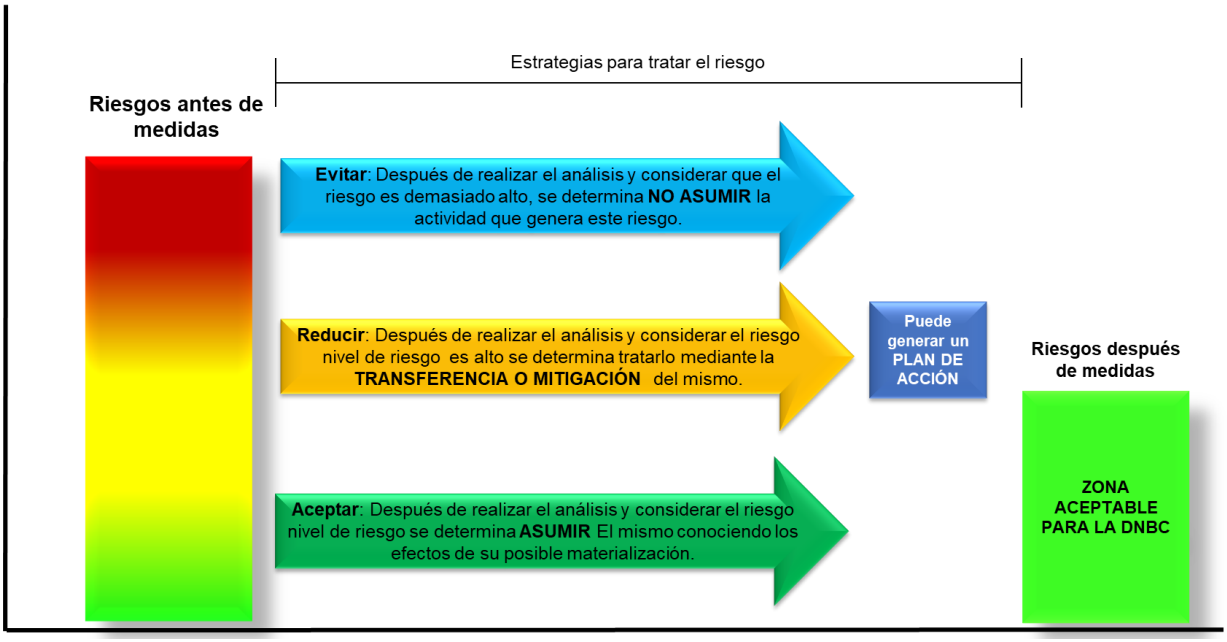
5.5. Tratamiento del riesgo

El resultado del nivel de riesgo (probabilidad por impacto) determina la estrategia a seguir por la entidad, las cuales son: aceptar, reducir o evitar. Esta decisión se toma frente al riesgo residual cuando se analizan los procesos en funcionamiento y frente al riesgo inherente cuando se trate de procesos nuevos.

Las estrategias de reducción se refieren a la definición de acciones de mitigación y transferencia del riesgo. La mitigación busca reducir la probabilidad de ocurrencia y/o severidad de impacto de un riesgo como, por ejemplo: prevención de pérdidas, manejo o administración de crisis o, planificación de la continuidad de los negocios; por lo que no necesariamente corresponde a un control adicional. Por su parte, la transferencia responde a acciones que trasladan a un tercero parte de la responsabilidad por el manejo de riesgos y/o la obligación por las consecuencias financieras del riesgo en caso de ocurrencia, como es el caso de la tercerización de servicios o la adquisición de seguros.

Para los riesgos asociados a posibles actos de corrupción, es claro que no admiten aceptación del riesgo, como se indica en el numeral 5.5.2. de esta política.

Ilustración 4: Estrategias para combatir el riesgo



Fuente: Elaboración propia

Las acciones de mitigación pueden generar un **PLAN DE ACCIÓN** esto dependerá del análisis que realice el Líder del Proceso con su equipo de trabajo. El plan de acción es una herramienta de planificación para la gestión y control de tareas o proyectos, el cual debe especificar:

a. Responsable: Nombre de quien será el responsable para ejecutar el plan.
b. Descripción: Es importante describir las actividades que contempla el plan de acción de manera secuencial, de tal manera que se pueda realizar su adecuado seguimiento.
c. Fecha de implementación: Fecha en la cual el plan estará en funcionamiento y se cuenta con la evidencia de su ejecución.
d. Fecha de seguimiento: Fecha en la cual se evaluará si el plan de acción mitigo de manera adecuada el riesgo.

5.5.1. Riesgo de gestión y seguridad de la información

La Dirección Nacional de Bomberos de Colombia determina las estrategias para combatir el riesgo de gestión y seguridad de la información de acuerdo con las zonas de riesgos identificadas en el mapa de calor y que son resultado del proceso de valoración del riesgo[1].

[1] Como se indicó en el numeral 4.5. la decisión de tratamiento al riesgo se toma a partir del resultado del riesgo residual

Las estrategias estarán encaminadas a priorizar el seguimiento de los riesgos ubicados en las zonas "Alta" y "Extrema"

Tabla 3: Acciones frente al nivel del Riesgo de Gestión y Seguridad de la Información

Zona de Riesgo	Acciones
Baja	**ACEPTAR**: no requiere de implementación de actividades de control. No obstante, la DNBC define controles que mitiguen las subcausas de los riesgos valorados en zona BAJA. El líder y gestor del proceso, cuando identifique un cambio en el riesgo o en las actividades que puedan afectar la valoración de sus riesgos debe reportarlo a la segunda línea de defensa. Los riesgos en zona baja pueden ser gestionados sin que se requiera la implementación de planes de acción, no obstante, semestralmente serán evaluados por el proceso de Gestión de Análisis y Mejora Continua para determinar si se han presentado cambios que requieran su ajuste en cuanto a su valoración de probabilidad y/o impacto.
Moderada	**REDUCIR:** se definen controles que mitiguen las subcausas de los riesgos, es decir que permitan reducir la probabilidad de ocurrencia y/o minimizar la severidad de su impacto. El líder y gestor del proceso deben realizar la autoevaluación mensual de donde se reporte la efectividad de las medidas de mitigación. Los riesgos en zona moderada pueden ser gestionados sin que se requiera la implementación de planes de acción, no obstante, semestralmente serán evaluados por el proceso de Gestión de Análisis y Mejora Continua para determinar si se han presentado cambios que requieran su ajuste en cuanto a su valoración de probabilidad y/o impacto.

cuando se analizan los procesos en funcionamiento y frente al riesgo inherente cuando se trate de procesos nuevos.

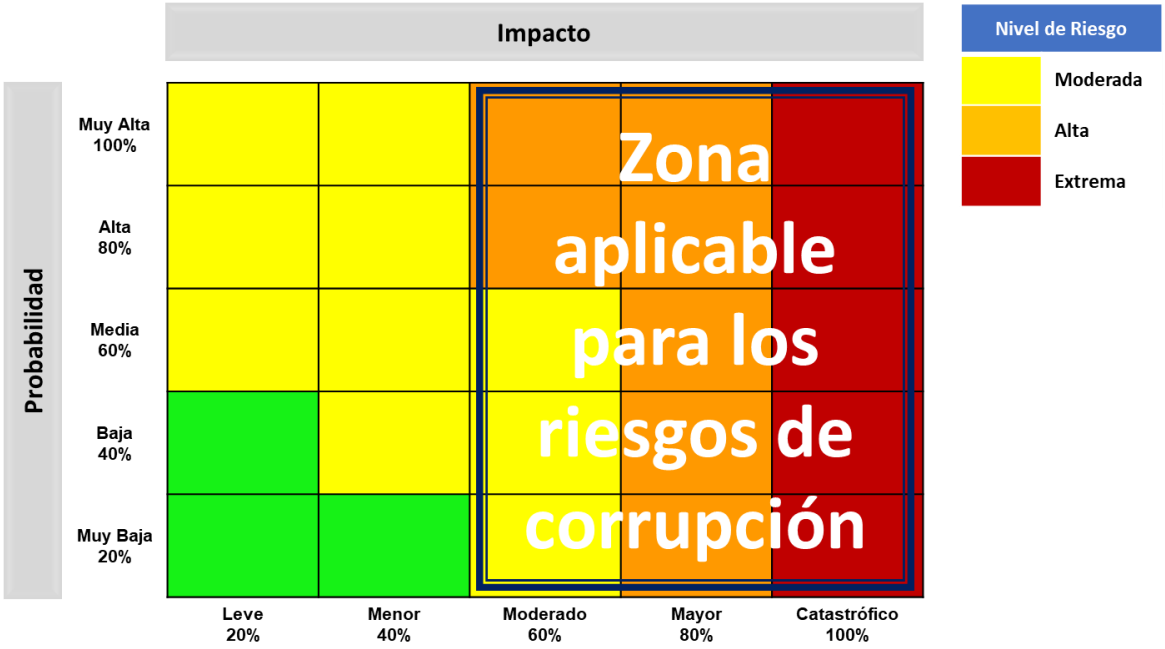
Zona de Riesgo	Acciones
Alta	**REDUCIR:** se definen controles que mitiguen las subcausas de los riesgos, es decir que permitan reducir la probabilidad de ocurrencia y/o minimizar la severidad de su impacto. El líder y gestor del proceso deben realizar la autoevaluación mensual de donde se reporte la efectividad de las medidas de mitigación, así como el avance de los planes de acción en riesgos, definidos en aquellos casos donde no existen medidas de mitigación o las medidas de mitigación no son efectivas. Gestión de Análisis y Mejora Continua realiza el seguimiento a los reportes de autoevaluación presentados por los procesos, con el fin de apoyar oportunamente en la construcción y/o rediseño de medidas de mitigación efectivas.
Extrema	Los riesgos en esta categoría pueden tomar las siguientes acciones. • **EVITAR:** se abandonan las actividades que dan lugar al riesgo, es decir, se decide no iniciar o continuar con la actividad puede generar que el riesgo se materialice. • **REDUCIR:** se definen controles que mitiguen las subcausas de los riesgos, es decir que permitan reducir la probabilidad de ocurrencia y/o minimizar la severidad de su impacto. El líder y gestor del proceso deben realizar la autoevaluación mensual de donde se reporte la efectividad de las medidas de mitigación, así como el avance de los planes de acción en riesgos, definidos en aquellos casos donde no existen medidas de mitigación o las medidas de mitigación no son efectivas. Gestión de Análisis y Mejora Continua realiza el seguimiento a los reportes de autoevaluación presentados por los procesos, con el fin de apoyar oportunamente en la construcción y/o rediseño de medidas de mitigación efectivas. Asimismo, realizará monitoreo mensual a los planes de acción de riesgos, notificado sus resultados al proceso de Gestión de Análisis y Mejora Continua, quien deberá verificar sus avances y reportar al Comité Directivo y el Comité Institucional de Coordinación de Control Interno los resultados para su seguimiento.

Fuente: Adaptación de la entidad, tomada de los conceptos definidos en la guía para la administración del riesgo y diseño de controles en entidades públicas, versión 5

5.5.2. Riesgo de corrupción

Para los riesgos de corrupción, el mapa de calor se reduce a las zonas moderadas, altas y extremas, como se muestra a continuación:

Ilustración 5: Nivel de Riesgo de Corrupción



Fuente: Gráfica adaptada de la guía para la administración del riesgo y diseño de controles en entidades públicas, versión 5 del DAFP

Al ser los riesgos de corrupción de alto impacto para la entidad no se acepta ningún riesgo, es decir que no se califican en zona de tolerancia baja y las estrategias de reducción deben tener un monitoreo continuo por parte de las líneas de defensa.

Por lo anterior, la Dirección Nacional de Bomberos de Colombia toma las siguientes decisiones sobre el tratamiento de los riesgos de corrupción:

Tabla 4: Acciones frente al Riesgo de Corrupción

Zona de Riesgo	Acciones
Moderada	**REDUCIR:** se definen controles que mitiguen las subcausas de los riesgos, es decir que permitan reducir la probabilidad de ocurrencia y/o minimizar la severidad de su impacto. El líder y gestor del proceso deben realizar la autoevaluación mensual de

Zona de Riesgo	Acciones
Moderada	donde se reporte la efectividad de las medidas de mitigación. Los riesgos en zona moderada pueden ser gestionados sin que se requiera la implementación de planes de acción, no obstante, semestralmente serán evaluados por el proceso de Gestión de Análisis y Mejora Continua para determinar si se han presentado cambios que requieran su ajuste en cuanto a su valoración de probabilidad y/o impacto.
Alta	**REDUCIR:** se definen controles que mitiguen las subcausas de los riesgos, es decir que permitan reducir la probabilidad de ocurrencia y/o minimizar la severidad de su impacto. El líder y gestor del proceso deben realizar la autoevaluación mensual de donde se reporte la efectividad de las medidas de mitigación, así como el avance de los planes de acción en riesgos, definidos en aquellos casos donde no existen medidas de mitigación o las medidas de mitigación no son efectivas. Gestión de Análisis y Mejora Continua realiza el seguimiento a los reportes de autoevaluación presentados por los procesos, con el fin de apoyar oportunamente en la construcción y/o rediseño de medidas de mitigación efectivas.
Extrema	Los riesgos en esta categoría pueden tomar las siguientes acciones. • **EVITAR:** se abandonan las actividades que dan lugar al riesgo, es decir, se decide no iniciar o continuar con la actividad puede generar que el riesgo se materialice. • **REDUCIR:** se definen controles que mitiguen las subcausas de los riesgos, es decir que permitan reducir la probabilidad de ocurrencia y/o minimizar la severidad de su impacto. El líder y gestor del proceso deben realizar la autoevaluación mensual de donde se reporte la efectividad de las medidas de mitigación, así como el avance de los planes de acción en riesgos, definidos en aquellos casos donde no existen medidas de mitigación o las medidas de mitigación no son efectivas. Gestión de Análisis y Mejora Continua realiza el seguimiento a los reportes de autoevaluación presentados por los procesos, con el fin de apoyar oportunamente en la construcción y/o rediseño de medidas de mitigación efectivas. Asimismo, realizará monitoreo mensual a los planes de acción en riesgos, notificado sus resultados al proceso de Gestión de Análisis y Mejora Continua, quien deberá verificar sus avances y reportar al Comité Directivo y el Comité Institucional de Coordinación de Control Interno los resultados para su seguimiento.

Fuente: Adaptación de la entidad, tomada de los conceptos definidos en la guía para la administración del riesgo y diseño de controles en entidades públicas, versión 5

5.6. Monitoreo

La DNBC reconoce la importancia del monitoreo de la Gestión del Riesgo, que comprende la verificación y vigilancia regular de la política y su metodología, para lo cual cada una de las líneas de defensa cumple un rol importante el cual se describe en el numeral 6.2.5 Monitoreo y Revisión del presente manual.

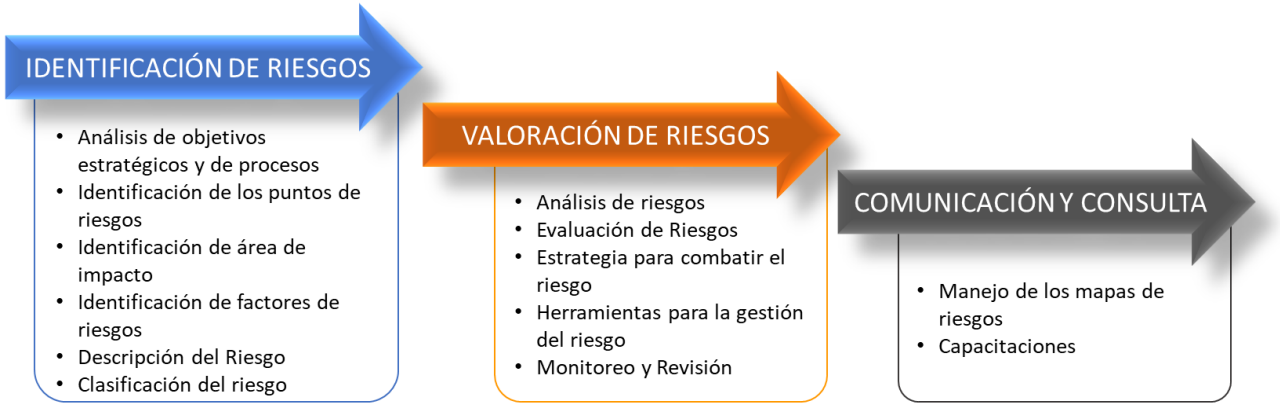
Siendo la primera línea de defensa, el primer responsable en la gestión del riesgo de la DNBC, serán los líderes y gestores de proceso los responsables en realizar el monitoreo de sus riesgos y controles, por medio de las herramientas dispuestas por la dirección, diseñadas por la segunda línea de defensa.

El monitoreo se realizará de acuerdo con la periodicidad de los controles, reportando de manera mensual los resultados de la autoevaluación de sus riesgos u controles.

6. DESARROLLO DE LA GESTIÓN DEL RIESGO EN LA DNBC

La política de riesgos de la entidad se complementa con las actividades para el análisis, identificación, evaluación, tratamiento y monitoreo, descritas en los pasos dos y tres de la metodología del DAFP, y que se complementan con la definición de estrategias de comunicación transversal a toda la entidad. Esto con el fin de lograr que la Gestión del Riesgo produzca los resultados esperados, es decir, el logro de los objetivos estratégicos de la entidad con la utilización óptima de sus recursos.

Ilustración 6: Pasos 2 y 3 de la metodología de la administración de riesgos del DAFP



Fuente: Adaptación propia

6.1. Identificación de riesgos

La base para la identificación de los riesgos está en el conocimiento y análisis de la entidad y su contexto, es por ello por lo que el primer paso es realizar un entendimiento de la misión, visión y objetivos estratégicos de la entidad, su articulación con la planeación institucional y su modelo de operación, que se despliega en la cadena de valor, el mapa de procesos y sus caracterizaciones.

Fuente: Imagen propia

6.1.1. Análisis de objetivos estratégicos

La Dirección Nacional de Bomberos de Colombia debe analizar los objetivos estratégicos e identificar los posibles riesgos que afecten su cumplimiento y que puedan ocasionar su éxito o fracaso, por lo que se hace necesario revisar si los objetivos estratégicos se encuentren alineados con la misión y visión institucional, así como, analizar su adecuada formulación, es decir, que contenga las características mínimas: específico, medible, alcanzable, relevante y proyectado en el tiempo.

6.1.2. Análisis de objetivos de procesos

Así mismo, los objetivos de proceso deben ser analizados con base en las características mínimas (específico, medible, alcanzable, relevante y proyectado en el tiempo) y además se debe revisar si están alineados con la misión y visión, es decir que contribuya a los objetivos estratégicos de la DNBC, para tal fin el líder junto con el gestor de proceso bebe analizar:

- Cómo el proceso contribuye al logro de la misión, visión y objetivos estratégicos de la entidad.
- Cuáles son los procesos con los cuales interactúa para lograr sus objetivos
- Quienes son las partes interesadas del proceso (a quien le ofrezco el servicio)

Por lo anterior debe conocer:

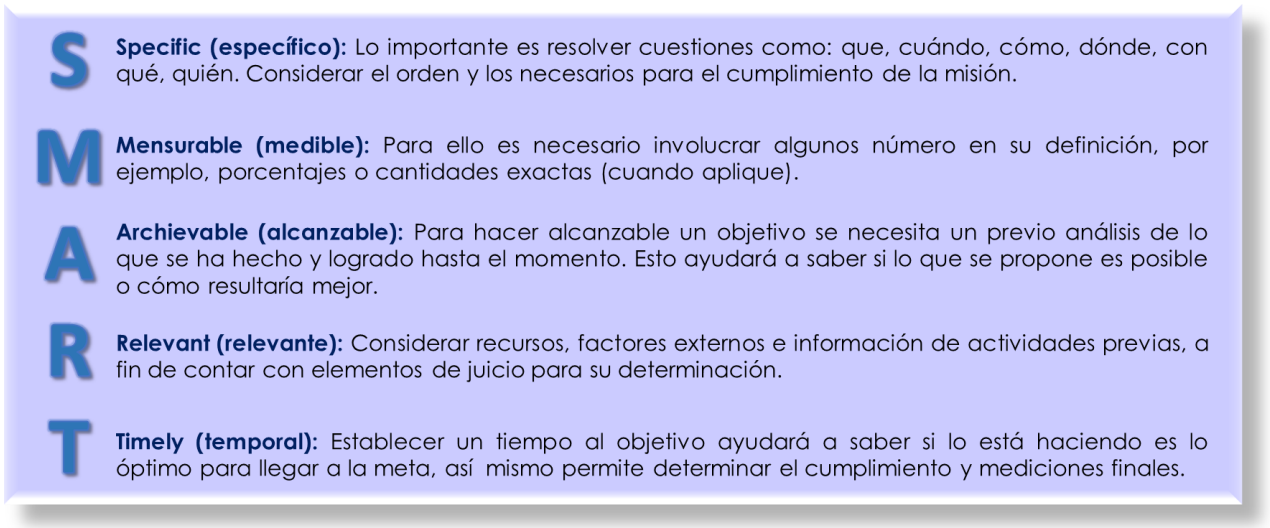
- La misión, visión y objetivos estratégicos
- El mapa de procesos
- La caracterización del proceso

Realizado este análisis el Líder del Proceso puede verificar si el objetivo es adecuado o debe ser replanteado.

6.1.3. Características mínimas para la definición de los objetivos

Para identificar si los objetivos estratégicos y de procesos se encuentren bien definidos, se debe verificar las características mínimas para su formulación, tomando como referente la metodología SMART[2].

Ilustración 7: Desglose características SMART



Fuente: Dirección de Gestión y Desempeño Institucional de Función Pública, 2020

6.1.4. Identificación del riesgo de gestión y de corrupción

La identificación del riesgo busca detectar las situaciones internas o externas que puedan afectar el logro de los objetivos del proceso, así como su repercusión en los objetivos institucionales, en esta etapa se debe establecer los factores de riesgos, las causas y sus consecuencias. Para ello se debe seguir los siguientes pasos:

1. **Análisis de los objetivos:** Antes de iniciar es importante que el proceso verifique si el objetivo de su proceso está alineado con la misión, visión y objetivos institucionales, para ello debe atender lo indicado en el numeral "6.1. Identificación de Riesgos" de este manual. En caso de no estar articulados, el líder del proceso junto con su equipo de trabajo debe reformular su objetivo atendiendo el procedimiento de control de documentos del Sistema de Gestión y reportarlo al proceso de Gestión de Análisis y Mejora Continua.
2. **Documentación preliminar:** para lograr un adecuado ejercicio de identificación es necesario contar con los insumos necesarios para realizar el ejercicio, el objetivo es identificar todas las situaciones que afecten el logro del objetivo del proceso, para ello revise:
   - La caracterización del proceso que le indica cuales son las entradas del proceso, las actividades y sus salidas.

[2] Hace referencia a las siglas en inglés que responden a: specific (específico), mensurable (medible), achievable (alcanzable), relevant (relevante), timely (temporal)

- Descripción de los procesos y/o flujos de proceso documentados
- Los planes de acción que le indican las metas definidas en el proceso para alcanzar los objetivos estratégicos.
- Planes de mejoramiento donde se ha identificado situaciones que deben ser atendidas por el proceso para mejorar su efectividad y eficiencia.
- Las obligaciones legales y de reporte que tiene el proceso y como está definida su ejecución para atenderlos oportunamente. No atenderlo deriva un riesgo de cumplimiento.
- Proyectos o nuevas actividades, es posible que dentro del proceso existan actividades que están en fase de diseño e implementación, es importante que a ese nivel también se revise el riesgo. Estos riesgos los definiremos como, riesgos de proyectos.

3. **Identificación puntos de riesgos:** Con un adecuado conocimiento del proceso, el equipo debe identificar en que parte del flujo o secuencia del proceso pueda existir situaciones que afecten su normal funcionamiento (eventos) y que deben mantenerse bajo control para asegurar que el proceso cumpla su objetivo de manera efectiva y eficiente.
4. **Identificación de las áreas de impacto:** A cada una de las situaciones identificadas en el paso anterior, se debe analizar cuál sería la consecuencia o impacto al que está expuesta la entidad. Las consecuencias pueden ser de carácter reputacional, que se refiere a la afectación del buen nombre de la entidad y de carácter económico que es cualquier afectación a su presupuesto.
5. **Identificación de factores de riesgos:** Se refiere a las fuentes generadoras de riesgos, es decir que son las circunstancia o situaciones que aumentan las probabilidades de que el riesgo se materialice. A continuación, se relacionan los factores o fuentes generadoras de riesgos en la operación de los procesos.

Tabla 5: Factores de Riesgos

Factor	Definición	Descripción
Procesos	Eventos relacionados con errores en las actividades que deben realizar los funcionarios y contratistas de la organización.	• Falta de procedimientos • Errores de grabación y/o autorización • Errores de cálculo para pagos internos y externos • Falta de capacitación en temas relacionados con el personal • Demoras en la entrega de información • Desconocimiento de la normatividad • Cambios normativos • Falta de seguimiento, supervisión y verificación • Ausencia del recurso humano
Talento	Incluye seguridad y salud	• Hurto de activos

Factor	Definición	Descripción
Humano	en el trabajo. Se analiza posible dolo e intención frente a corrupción.	• Posibles comportamientos no éticos de los empleados • Fraude interno (corrupción, soborno) • Falta de idoneidad, experticia y conocimiento
Tecnología	Eventos relacionados con la infraestructura tecnológica de la entidad.	• Daño de equipos • Caída de la aplicación • Caída de redes • Errores de programas
Infraestructura	Eventos relacionados con la infraestructura física de la entidad.	• Derrumbes • Incendios • Inundaciones • Daños a activos físicos
Evento externo	Situaciones externas que afectan la entidad.	• Suplantación de identidad • Asalto a la oficina • Atentados, vandalismo, orden público • Escasez en los recursos económicos y financieros otorgados a la DNBC para su ejecución.

Fuente: Tabla tomada de la guía para la administración del riesgo y diseño de controles en entidades públicas, versión 5.

Para los riesgos de gestión y seguridad de la información, se indicará en el mapa de riesgos el factor o factores de riesgos asociados a los riesgos identificados por la Dirección, de manera que permita realizar un mejor análisis para la definición de las medidas de mitigación.

6. **Descripción del Riesgo:** La descripción del riesgo contiene todos los detalles que sean necesarios y que sean fácil de entender tanto para el líder del proceso como para las personas ajenas al proceso. Para su descripción se adaptó las instrucciones de Función Pública, que se describe a continuación.

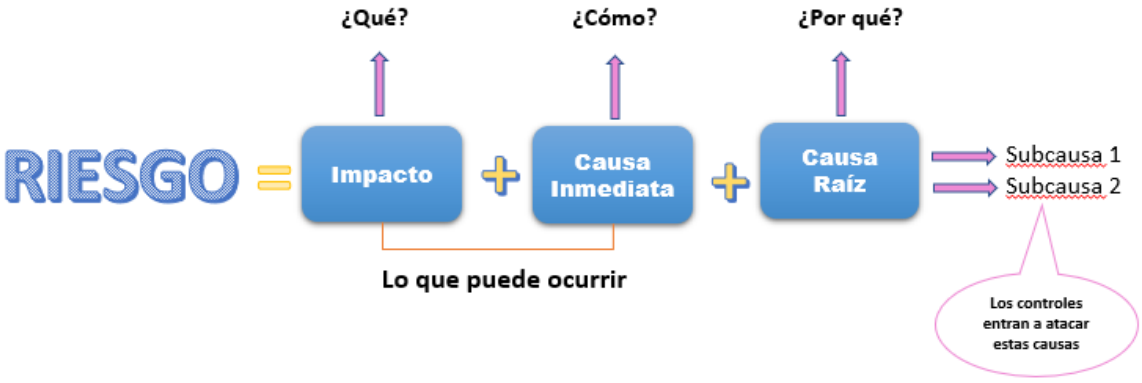
   ✓ **Impacto:** Las consecuencias que puede ocasionar a la DNBC la materialización del riesgo.

   ✓ **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:** es la causa principal o básica, corresponden a las razones por las cuales se puede presentar el riesgo, son la base para la definición de controles en la etapa de valoración del riesgo. Se debe tener en cuenta que para un mismo riesgo puede

existir más de una causa o subcausas que pueden ser analizadas.

Ilustración 8: Estructura para la redacción del riesgo



Fuente: Ilustración tomada de la guía para la administración del riesgo y diseño de controles en entidades públicas, versión 5.

Ejemplo:

- Proceso: Atención al Usuario
- Objetivo: Gestionar dentro de los términos de Ley, los requerimientos formulados por la ciudadanía y grupos de interés, para satisfacer sus necesidades, mediante la orientación y atención de peticiones, quejas, reclamos, sugerencias y denuncias, así como evaluar la percepción de los servicios y tramites ofrecidos por la DNBC.
- Alcance: Inicia con la presentación de las solicitudes de trámites, servicios, peticiones, quejas, reclamos y sugerencias por parte de las partes interesadas a través de canales telefónica, virtual y presencial y termina con la prestación de los servicios o atención de las PQRSD y la medición de la percepción de los usuarios frente a la prestación de los servicios.

Atendiendo el esquema propuesto para la redacción del riesgo, tenemos:

Tabla 6: Elementos descriptivos del riesgo

Inicia con	Impacto (¿Qué?)	Causa Inmediata (¿Cómo?) Situación evidente – el cómo se materializa el impacto identificado	Causa raíz (¿Por qué?) Razones por las cuales se puede materializar el riesgo
Posibilidad de	Afectación económica y reputacional	Por pérdida del buen nombre ante sanciones disciplinarias a funcionarios y/o contratistas	Debido a la inoportunidad y/o incumplimiento en la respuesta PQRSD

Fuente: Elaboración propia

Premisas para una adecuada redacción del riesgo

- No describir como riesgos omisiones ni desviaciones del control.

  Ejemplo: errores en la liquidación de la nómina por fallas en los procedimientos existentes.

- No describir causas como riesgos.

  Ejemplo: inadecuado funcionamiento de la plataforma estratégica donde se realiza el seguimiento a la planeación.

- No describir riesgos como la negación de un control.

  Ejemplo: retrasos en la prestación del servicio por no contar con digiturno para la atención.

- No existen riesgos transversales, lo que pueden existir son causas transversales.

Ejemplo: pérdida de expedientes. Puede ser un riesgo asociado a la gestión documental, a la gestión contractual o jurídica y en cada proceso sus controles son diferentes.

7. **Clasificación del Riesgo:** La clasificación permite agrupar los riesgos por categorías para un mejor análisis y tratamiento, ya que esta actividad permitirá detectar riesgos transversales en toda la entidad. Así mismo la categorización ayuda a la definición de estrategias para su mitigación y la toma de decisiones a nivel estratégico.

Tabla 7: Clasificación de riesgos de la DNBC

CATEGORÍA	DESCRIPCIÓN
Ejecución y administración de procesos	Pérdidas derivadas de errores en la ejecución y administración de procesos.
Relaciones Laborales	Pérdidas que surgen de acciones contrarias a las leyes o acuerdos de empleo, salud o seguridad, del pago de demandas por daños personales o discriminación.
Usuarios, productos y prácticas	Fallas negligentes o involuntarias de las obligaciones frente a los usuarios y que impiden satisfacer una obligación profesional frente a éstos.
Fraude Externo	Pérdida derivada de actos de fraude por personas ajenas a la organización (no participa personal de la entidad)
Fraude Interno	Pérdida debido a actos de fraude, actuaciones irregulares, comisión de hechos delictivos abuso de confianza, apropiación indebida, incumplimiento de regulaciones legales o internas de la entidad en las cuales está involucrado por lo menos un participante interno de la organización, son realizada de forma intencional y/o con ánimo de lucro para sí mismo o terceros.
Fallas Tecnológicas	Errores en hardware, software, telecomunicaciones, interrupción de servicios básicos.
Daños a activos fijos/eventos externos	Pérdida por daños o extravíos de los activos fijos por desastres naturales u otros riesgos/eventos externos como atentados, vandalismo, orden público.

Fuente: Tabla adoptada de la guía para la administración del riesgo y diseño de controles en entidades públicas, versión 5, de acuerdo con los criterios de la DNBC para clasificar sus riesgos.

Para los riesgos de gestión y seguridad de la información, se indicará en el mapa de riesgos la categoría del riesgo identificado, que permita hacer análisis por categorías para la definición de estrategias.

6.1.5. Características especiales en la identificación del riesgo de corrupción

Los riesgos de corrupción están dentro del marco del Plan Anticorrupción y de Atención al Ciudadano establecido en el artículo 73 de la Ley 1474 de 2011 y el artículo 2.1.4.1 del Decreto 124 de 2016 que define las estrategias de lucha contra la corrupción y de atención al ciudadano, el cual se articula con los demás componentes establecidos para el desarrollo del plan, ya que se trata de una acción integral en la lucha contra la corrupción.

Ilustración 9: Componentes del plan anticorrupción y atención al ciudadano

Fuente: Elaboración conjunta entre Dirección de Gestión y Desempeño Institucional de Función Pública y la Secretaría de Transparencia

El riesgo de corrupción es la posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado. "Esto implica que las prácticas corruptas son realizadas por actores públicos y/o privados con poder e incidencia en la toma de decisiones y la administración de los bienes públicos" (Conpes N° 167 de 2013).

Para la adecuada identificación de estos riesgos es importante tener encienta que corresponden a la posibilidad de que, por la acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado, por lo tanto, para facilitar la identificación de riesgos de corrupción y evitar que se presenten confusiones entre un riesgo de gestión y uno de corrupción, se recomienda una vez identificado, verificar si cumple con las siguientes características:

- **Acción u omisión:** El riesgo responde a una posible acción u omisión por parte del funcionario o servidor.
- **Uso de poder:** El riesgo se materializa por el uso de poder de quien ejecuta la acción generadora del riesgo.
- **Desviar la gestión de lo público:** No cumple con la gestión del proceso, por lo que se desvía de su objetivo.
- **Beneficio Privado:** Se busca beneficiar a un tercero ante el acto u omisión de la acción generadora del riesgo.

En ese mismo sentido, para una mejor identificación es importante considerar los siguientes aspectos:

- El riesgo de corrupción se define como la posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.
- Los riesgos de corrupción se establecen sobre procesos.
- El riesgo debe estar descrito de manera clara y precisa. Su redacción no debe dar lugar a ambigüedades o confusiones con la causa generadora de los mismos.

Con el fin de facilitar la identificación de riesgos de corrupción y evitar que se presenten confusiones entre un riesgo de gestión y uno de corrupción, se sugiere la utilización de la matriz de definición de riesgo de corrupción, que incorpora cada uno de los componentes de su definición. De acuerdo con la siguiente matriz, si se marca con una X en la descripción del riesgo que aparece en cada casilla quiere decir que se trata de un riesgo de corrupción:

Tabla 8: Matriz para la definición de riesgos de corrupción

Descripción del Riesgo	Acción u omisión	Uso de poder	Desviar la gestión de lo público	Beneficio privado
Posibilidad de recibir o solicitar cualquier dádiva o beneficio a nombre propio o de terceros con el fin de celebrar un contrato.	X	X	X	X

Fuente: Secretaría de Transparencia de la Presidencia de la República

TENGA EN CUENTA

Las preguntas clave para la identificación del riesgo son:

¿Qué puede suceder? ¿Cómo puede suceder?

¿Cuándo puede suceder? ¿Qué consecuencias tendría su materialización?

A manera de ilustración se señalan algunos de los procesos susceptibles de actos de corrupción, a partir de los cuales se podrán adelantar análisis de contexto interno para la adecuada identificación del riesgo.

Tabla 9: Procesos o actividades susceptibles de riesgo de corrupción

Direccionamiento estratégico (alta dirección)	• Concentración de autoridad o exceso de poder. • Extralimitación de funciones • Ausencia de canales de comunicación • Amiguismo y clientelismo
Financiero	• Inclusión de gastos no autorizados • Inversiones de dineros públicos en entidades de dudosa solidez financiera • Beneficios indebidos para servidores públicos encargados de la administración de inversiones • Inexistencia de registros auxiliares que permitan identificar y controlar rubros de inversión • Inexistencia de archivos contables • Afectación de rubros que no corresponden con el objeto del gasto en beneficio propio o cambio de una retribución económica • Manipulación de información para el pago de partidas con otorgamiento de beneficios a terceros ficticios o que no corresponden.
De contratación **De contratación**	• Estudios previos o de factibilidad deficientes • Estudios previos o de factibilidad manipulados por personal interesado en el futuro proceso de contratación • Pliegos de condiciones hechos a la medida de una firma en particular • Disposiciones establecidas en los pliegos de condiciones que permiten a los participantes direccionar los procesos hacia un grupo en particular • Visitas obligatorias establecidas en el pliego de condiciones que restringen la participación. • Adendas que cambian condiciones generales del proceso para favorecer a grupos determinados. • Urgencia manifiesta inexistente. • Concentrar las labores de supervisión en poco personal • Contratar con compañías de papel que no cuentan con experiencia
De información y documentación	• Ausencia o debilidad de medidas y/o políticas de conflictos de interés. • Concentración de información de determinadas actividades o

	procesos en una persona. • Ausencia de sistemas de información que pueden facilitar el acceso a información y su posible manipulación o adulteración. • Ocultar la información considerada pública para los usuarios. • Ausencia o debilidad de canales de comunicación
De investigación disciplinaria	• Inexistencia de canales de denuncia interna o externa. • Dilatar el proceso para lograr el vencimiento de términos o la prescripción de este. • Desconocimiento de la ley mediante interpretaciones subjetivas de las normas vigentes para evitar o postergar su aplicación. • Exceder las facultades legales en los fallos.

Fuente: Secretaría de Transparencia

Generalidades acerca de los riesgos de Corrupción

- El mapa de riesgos de corrupción se actualiza anualmente y es responsabilidad de los líderes de proceso junto con su equipo de trabajo.
- La consolidación del mapa de riesgos de corrupción le corresponde al proceso de planeación estratégica quien hace las veces de la oficina de planeación.
- El mapa de riesgos de corrupción se debe publicar en la página web de la entidad, en la sección de transparencia y acceso a la información pública que establece el artículo 2.1.1.2.1.4 del Decreto 1081 de 2015 o en un medio de fácil acceso al ciudadano, a más tardar el 31 de enero de cada año. La publicación será parcial y fundamentada en la elaboración del índice de información clasificada y reservada. En dicho instrumento la entidad debe establecer las condiciones de reserva y clasificación de algunos de los elementos constitutivos del mapa de riesgos en los términos dados en los artículos 18 y 19 de la Ley 1712 de 2014. En este caso se deberá anonimizar esa información. Es decir, la parte clasificada o reservada, aunque se elabora, no se hace visible en la publicación. Recuerde que las excepciones solo pueden estar establecidas en la ley, un decreto con fuerza de ley o un tratado internacional ratificado por el Congreso o en la Constitución.
- Los servidores públicos y contratistas de la entidad deben conocer el mapa de riesgos de corrupción antes de su publicación. Para lograr este propósito la oficina de planeación o quien haga sus veces, deberá diseñar y poner en marcha las actividades o mecanismos necesarios para que los funcionarios y contratistas conozcan, debatan y formulen sus apreciaciones y propuestas sobre el proyecto del mapa de riesgos de corrupción. Así mismo, dicha oficina adelantará las acciones para que la ciudadanía y los interesados externos conozcan y manifiesten sus consideraciones y sugerencias sobre el proyecto del mapa de riesgos de corrupción. Deberá dejarse la evidencia del proceso de socialización y publicarse sus resultados.
- Ajustes y modificaciones: se podrán llevar a cabo los ajustes y modificaciones necesarias orientadas a mejorar el mapa de riesgos de corrupción después de su publicación y durante el respectivo año de vigencia. En este caso deberán dejarse por escrito los ajustes,

modificaciones o inclusiones realizadas.

- Monitoreo: en concordancia con la cultura del autocontrol al interior de la entidad, los líderes de los procesos junto con su equipo realizarán monitoreo y evaluación permanente a la gestión de riesgos de corrupción.
- Seguimiento: el jefe de control interno o quien haga sus veces debe adelantar seguimiento a la gestión de riesgos de corrupción. En este sentido es necesario que en sus procesos de auditoría interna analice las causas, los riesgos de corrupción y la efectividad de los controles incorporados en el mapa de riesgos de corrupción

6.1.6. Características especiales en la identificación del riesgo de seguridad de la información

Para la identificación de los riesgos de seguridad de la información, la DNBC seguirá los procedimientos descritos en el Anexo 4 Modelo nacional de riesgos de seguridad de la información para entidades públicas del Ministerio de las Tecnologías de la información y las comunicaciones y gestionará los riesgos de los activos que tengan un nivel de criticidad "alto", según lo descrito en el Capítulo 7 Riesgos de Seguridad de la Información, de este manual.

6.2. Valoración del riesgo

Comprende las actividades que en conjunto le permite a la Dirección Nacional de Bomberos de Colombia conocer las situaciones o eventos que pueden afectar el logro de sus objetivos y que, al priorizarlos de acuerdo con la probabilidad de ocurrencia e impacto, facilita la toma de decisiones para el logro de los objetivos de la entidad.

6.2.1. Análisis de riesgos

Busca establecer la probabilidad e impacto del riesgo analizado, con el fin de determinar la zona de riesgo inicial en que se encuentra ubicado, se le conoce como riesgo inherente y permite que la entidad conozca los riesgos que de manera intrínseca[3] se presentan en los procesos para definir las acciones o controles a seguir para su gestión.

1. **Determinar la probabilidad:** La probabilidad mide la posibilidad de que el riesgo se llegue a suceder, se mide entre 0 y 1 y permite determinar que riesgos son más susceptibles a materializarse. Adoptando la metodología del DAFP la probabilidad se determinará por el número de veces que se pasa por el punto de riesgo en el periodo de un año; por ejemplo, si analizamos un riesgo asociado al proceso de contratación su probabilidad estará dada por el número de veces que en el año se suscriben contratos, es decir entre más se ejecute la actividad se incrementa la posibilidad de que el riesgo se materialice. Para determinar la probabilidad utilice la tabla definida en el numeral 5.3. Niveles para calificar la probabilidad, definido en este manual.
2. **Determinar el impacto:** El impacto determina el efecto que generaría en la entidad el riesgo al materializarse, medido por la pérdida económica y reputacional. Es así como el líder del proceso junto con su equipo de trabajo debe analizar si, el riesgo al materializarse generaría pérdidas económicas y/o reputacionales y de acuerdo con este análisis,

[3] Por el simple hecho de existir el riesgo está presente.

determinar el grado de afectación para lo cual se utiliza la tabla definida en el numeral 5.4. Niveles para calificar el impacto, definido en este manual.

Para los riesgos de corrupción el impacto es medido considerando la siguiente tabla, la cual el líder del proceso junto con su gestor debe analizar.

Tabla 10: Criterios para calificar el impacto en riesgos de corrupción

No.	Pregunta: SI EL RIESGO DE CORRUPCIÓN SE MATERIALIZA PODRÍA	RESPUESTA	
		SI	NO
1	¿Afectar al grupo de funcionarios del proceso?		
2	¿Afectar el cumplimiento de metas y objetivos de la dependencia?		
3	¿Afectar el cumplimiento de la misión de la entidad?		
4	¿Afectar el cumplimiento de la misión del sector al que pertenece la entidad?		
5	¿Generar pérdida de confianza en la entidad, afectando su reputación?		
6	¿Generar pérdida de recursos económicos?		
7	¿Afectar la generación de productos o la prestación de servicios?		
8	¿Dar lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien, servicios o 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 la credibilidad del sector?		
16	¿Ocasionar lesiones físicas o pérdidas de vidas humanas?		
17	¿Afectar la imagen regional?		
18	¿Afectar la imagen nacional?		
19	¿Generar daño ambiental?		
RESULTADOS:			

No.	Pregunta: SI EL RIESGO DE CORRUPCIÓN SE MATERIALIZA PODRÍA	RESPUESTA	
		SI	NO
• De UNO a CINCO preguntas afirmativas genera un impacto MODERADO • De SEIS a ONCE preguntas afirmativas genera un impacto ALTO o MAYOR • De DOCE a DIECINUEVE preguntas afirmativas genera un impacto EXTREMO o CATASTRÓFICO			

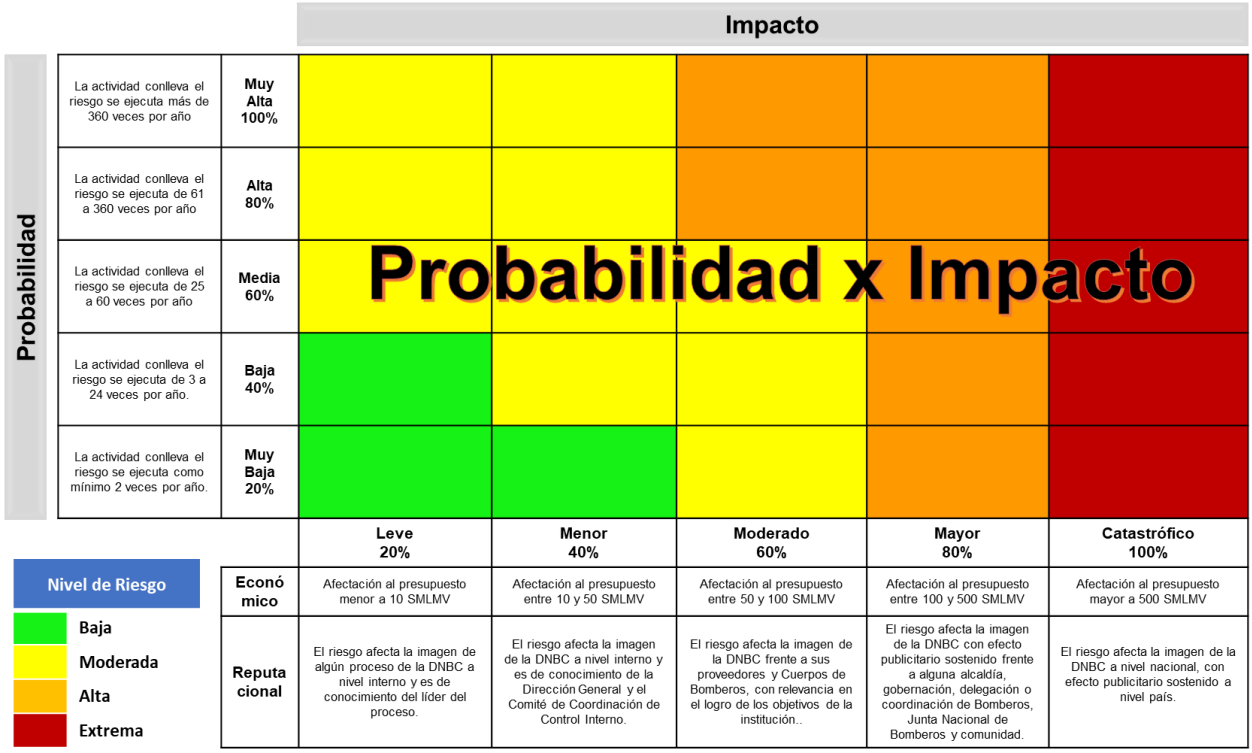
Fuente: Tabla adoptada de la guía para la administración del riesgo y diseño de controles en entidades públicas, versión 5, de acuerdo con los criterios de la DNBC para clasificar sus riesgos.

Tenga en cuenta:

- Para determinar la probabilidad y el impacto del riesgo se debe emplear las tablas definidas por la DNBC para su valoración.
- El riesgo puede tener afectación económica y reputacional, en esos casos se debe analizar la valoración para las dos afectaciones y el valor final será el que resulte más alto.
- La valoración del riesgo debe realizarla el Líder del proceso junto con su gestor, quienes conocen sus procesos y actividades, ya que esta nueva metodología no es subjetiva y no da lugar a percepciones de diferentes expertos.
- Para los riesgos de corrupción el impacto debe analizarse con la Tabla No. 11 "Criterios para calificar el impacto en riesgos de corrupción", para la probabilidad se utiliza la tabla de probabilidad definida en este manual.

El cruce del análisis de la probabilidad e impacto del riesgo, de acuerdo con los niveles definidos por la entidad en el capítulo 5 de este manual, el resultado determina la zona de riesgo inicial, o riesgo inherente, es decir, sin considerar los controles.

Ilustración 10: Matriz de Calor (niveles de severidad del riesgo)



Fuente: Adaptación propia

6.2.2. Evaluación del riesgo

La evaluación del riesgo busca confrontar los resultados del análisis del riesgo inicial, conocido también como **Riesgo Inherente,** frente a los controles establecidos, con el fin de determinar la zona de riesgo final o **Riesgo Residual.**

Identificación y diseño de controles

El control es la medida que permite reducir o mitigar el riesgo, es decir que responde a las actividades, herramientas y estrategias implementadas por el proceso para gestionar la causa raíz por la cual se puede materializar el riesgo, por lo que la identificación adecuada de los riesgos ayuda a un diseño efectivo de medidas de control.

La identificación es responsabilidad del líder del proceso, quien en conjunto con sus gestores y equipo de trabajo analizan el flujo de actividades e identifican las medidas que permiten mitigar el riesgo, este trabajo se hace a criterio de expertos.

Así como en la identificación de riesgos, una vez se identifique la medida de control se debe realizar su diseño, es decir su adecuada redacción. Esto busca que los controles sean entendibles para todo el equipo de trabajo, así como para externos. Servirá también para que los controles se ejecuten de manera adecuada y no se presenten desviaciones más adelante.

Los elementos que comprende la estructura del control para su adecuado diseño son:

- **Objetivo del control:** Corresponde al propósito por el cual se implementa el control, cuál es su función en la mitigación del riesgo**.**
- **Responsable de ejecutar el control:** identifica el cargo del funcionario que ejecuta el control, en caso de que sea un control que se ejecuta de manera automática se identifica el sistema por el cual se realiza la actividad.
- **Frecuencia:** describe la periodicidad en la cual se ejecuta la acción durante el año, estas pueden ser: Anual, Semestral, Cuatrimestral, Trimestral, Bimestral, Mensual, Quincenal, Diaria, Más que Diaria o cuando se requiera, esta última debe describirse en detalle cual es la circunstancia genera que se ejecute el control.
- **Acción**: determina la actividad que ejecuta el control mediante un verbo.
- **Complemento**: descripción detallada de cómo se ejecuta la acción, clave para que sea entendido por el ejecutor del control y que pueda ser replicado por otro servidor o contratista en caso de una contingencia. Así mismo se debe indicar qué pasa con las observaciones o desviaciones resultantes de ejecutar el control.
- **Evidencia**: descripción del rastro que el control deja al ser ejecutado, como formatos, autorizaciones, actas, reportes del sistema, entre otros. Es necesario para verificar su ejecución en un determinado periodo de tiempo y asegura el adecuado funcionamiento del proceso.

Tabla 11: Ejemplo de la redacción de un control

Objetivo del Control	Asegurar que la información recibida por parte del proveedor cumpla con los requisitos establecidos en Ley de Contratación.
Responsable	El profesional de contratación
Frecuencia	Cada vez que se contrata
Acción	Verifica que la información suministrada por el proveedor corresponda con los requisitos establecidos acorde con el tipo de contratación,
Complemento	A través de una lista de chequeo donde están los requerimientos de información y la revisa con la información física suministrada por el proveedor, los contratos que cumplen son registrados en el sistema de información de contratación, los que no se suspende el proceso hasta que se complete la información o se cambie de proveedor.
Evidencia	Lista de verificación y soportes del proveedor consignado en la carpeta de contratación.

Fuente: Tabla adoptada de la guía para la administración del riesgo y diseño de controles en entidades públicas, versión 5.

También es importante identificar si las medidas ayudarán a mitigar la probabilidad o el impacto del riesgo y en qué momento se ejecuta, es decir antes de que se materialice el riesgo o una vez haya ocurrido, a continuación, se define:

Tabla 12: Clasificación de Controles

Ciclo	Clase	Función	Ejemplos
Entradas Recursos que requiere el proceso	**Preventivo** Va a las causas del riesgo generalmente atacan la probabilidad	• Impedir que ocurra un error, una omisión o acto malicioso • Monitorear tanto las operaciones como el ingreso de datos • Tratar de predecir problemas potenciales antes de que estos ocurran y hacer ajustes	• Emplear solo personal calificado • Segregar funciones • Documentos bien diseñados (Prevenir errores) • Procedimientos adecuados para la autorización de transacciones
Interrelaciones Actividades que permiten transformas las entradas en productos y/o servicios	**Detectivos** Detecta algo que ocurre y devuelve el proceso a los controles preventivos. Atacan la probabilidad	• Detectar problemas antes de que surjan	• Sistemas de acceso físico a las instalaciones • Control de totales en la contabilidad. • Mensajes de error en el sistema
Salidas Productos y/o servicios del proceso	**Correctivos** Atacan el impacto frente a la materialización del riesgo	• Reportar que ha ocurrido un error una omisión o un acto malicioso • Remediar problemas descubiertos por controles detectivos • Minimizar el impacto de una amenaza	• Planeación de contingencias • Procedimientos de respaldo, como backups • Revisiones de la Gerencia

Fuente: Tabla que integra el ciclo del procesos y tipologías de controles presentado en la guía para la administración del riesgo y diseño de controles en entidades públicas, versión 5 con ejemplos para su comprensión.

Por último, debemos registrar de qué manera se ejecuta el control:

- **Control Manual**: son ejecutados por personas.
- **Control Automático**: son ejecutados por un sistema.

Análisis y evaluación de controles de gestión y seguridad de la información

Para verificar si los controles mitigan el riesgo de la manera esperada es necesario analizarlos y realizar una evaluación sobre los mismos. Para ello se tendrán en cuenta los siguientes elementos a los cuales se les da un valor de acuerdo con las características de la DNBC, como se muestra a continuación.

Tabla 13: Atributos para evaluar el diseño del control

Característica			Peso
Atributos de eficiencia (65%)	Tipo	Preventivo	20%
		Detectivo	10%
		Correctivo	5%
	Implementación	Automático	20%
		Manual	10%
Atributos informativos (35%)	Documentación	Documentado	15%
		Sin documentar	5%
	Frecuencia	Continua	10%
		Aleatoria	0%
	Evidencia	Con registro	5%
		Sin registro	0

Fuente: adaptación propia

Para la DNBC es importante valorar los atributos informativos de los controles, ya que dichos atributos permiten definir su diseño, asegurando la continuidad a las actividades ante cambios en los ejecutores.

Así mismo la DNBC considerará en la evaluación del riesgo, la evaluación de la efectividad del control, que refiere a que se está ejecutando de manera adecuada y que su ejecución permite mitigar el riesgo. Para calificar la efectividad del control en el mapa de riesgos, se tomarán los resultados de las autoevaluaciones realizadas por los líderes y gestores de proceso, los monitoreos realizados por el proceso de Gestión de Análisis y Mejora Continua y, las evaluaciones realizadas por el proceso de Evaluación y Seguimiento, quienes de acuerdo con sus roles y responsabilidades en la DNBC podrán determinar si el control es efectivo, requiere mejora o es inefectivo.

Para determinar si el control es efectivo, por mejorar o no efectivo, se consideran los siguientes criterios que deben ser tenidos en cuenta por las tres líneas de defensa:

Tabla 14: Criterios para calificar el control

CRITERIO	DESCRIPCIÓN

Efectivo	Se considera que el control es efectivo cuando: a. No se han materializado riesgos asociados al control analizado. La Dirección no se ve afectada en su imagen y/o patrimonialmente. b. El proceso conoce el control y demuestra su ejecución con la evidencia adecuada. a. La periodicidad es adecuada para mitigar el riesgo. b. El responsable de ejecutar el control tiene autoridad para tomar decisiones en caso de desviaciones.
Por Mejorar	Cuando se identifica que el control puede ser fortalecido, debido a alguna de las siguientes situaciones: a. El control se ejecuta y está claro por sus ejecutores, no obstante, no se guarda siempre la evidencia de su ejecución. b. Se videncia que el procedimiento documentado no está actualizado, por lo que el control que opera descrito en el mapa de riesgos es diferente al que está documentado en el procedimiento del proceso. c. Si bien el control se ejecuta, se ha identificado buenas prácticas o referentes de otras entidades que pueden ser considerados en el proceso.
No Efectivo	Cuando producto del análisis del control se identifica que este no ayuda a mitigar el riesgo debió a alguna de las siguientes situaciones: a. Se ha materializado el riesgo asociado al control. La Dirección se ve afectada en su imagen y/o patrimonialmente. b. La periodicidad en que se determinó su ejecución no ayuda a prevenir la ocurrencia del riesgo. c. El proceso no ejecuta el control de acuerdo con lo que está escrito en el mapa de riesgos, es decir no se ejecuta de acuerdo con su diseño. d. El responsable que realiza el control no es adecuado, ya que de acuerdo con el control descrito no cuenta con la autoridad suficiente para tomar decisiones en caso de desviaciones.
No evaluado	Se considera no evaluado cuando: a. La fecha de seguimiento es inferior a la fecha en que se debe aplicar. b. Se trata de un control que el proceso diseña por cambio de una estrategia o como respuesta a un plan de acción o mejoramiento, no podemos determinar si este realmente mitiga el riesgo, ya que aún no se ha ejecutado. Por tal motivo ninguna de las líneas de defensa puede determinar si el control es efectivo o no.

Valorar la efectividad permite al proceso determinar las estrategias de mejoramiento para una adecuada mitigación de las causas generadoras, por consiguiente:

a. Si un control **no es efectivo** el proceso deberá generar un plan de acción de mejoramiento.
b. Si el control **está por mejorar** el proceso deberá evaluar si es necesario generar un plan de acción de mejoramiento y reportar su resultado al proceso de Gestión de Análisis y Mejora Continua, quien validará la decisión.

Tabla 15: Porcentaje de calificación frente a la efectividad del control

DESCRIPCIÓN	%
Efectivo	100%
Por Mejorar	60%
No Efectivo	0%
No evaluado	No Aplica

Por consiguiente, el control será recalibrado con los porcentajes descritos en la tabla anterior, de acuerdo con el análisis realizado por la línea de defensa, que hubiera hecho el análisis.

Cuando el control esté analizado por más de una línea de defensa, se tomará el resultado con mayor criticidad. Es decir, si producto del análisis de un control, la primera línea de defensa en su autoevaluación considera que el control es efectivo, la segunda línea en su monitoreo identifica que es inefectivo y la tercera en su evaluación indica que es efectivo, el control será evaluado como inefectivo.

Definición del riesgo residual para riesgos de gestión y seguridad de la información

El riesgo residual es el valor resultante de aplicar las medidas de mitigación implementadas sobre determinado riesgo.

Por lo general los riesgos tiene establecidos más de una acción de mitigación, ya que estas siempre se diseñan para atacar las causas raíz del riesgo, por lo que para determinar el riesgo residual se debe:

1. Determinar el peso o valor de cada control de acuerdo con lo definido en la Tabla no. 10. Atributos para evaluar el diseño del control.
2. Identificar si la medida ataca la probabilidad de ocurrencia o el impacto del riesgo.
3. Por medida y dimensión atacada (probabilidad de ocurrencia o impacto) se realiza el cálculo de reducción.
4. Esto dará un valor final que determina el nievo nivel de riesgo residual

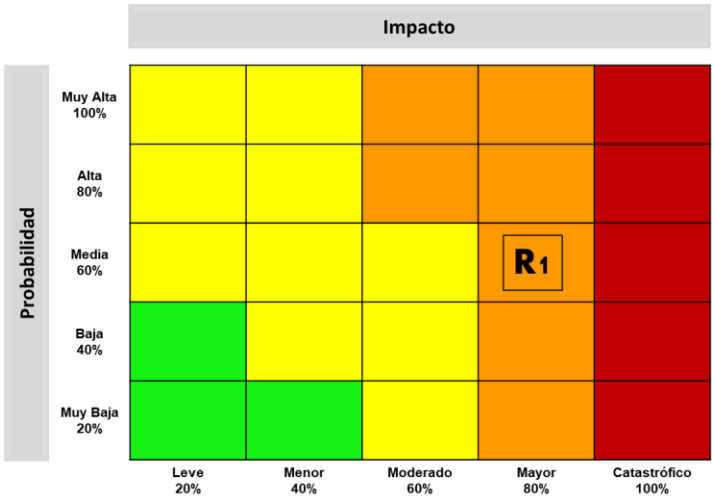
Los anteriores pasos estarán programados en plantillas Excel para la facilidad de los gestores y los líderes de proceso, no obstante, se presenta el ejemplo de la Guía para la administración del riesgo y diseño de controles en entidades públicas, versión 5, del Dirección de Gestión y Desempeño Institucional de Función Pública para una mejor comprensión.

Ejemplo:

Proceso Gestión de Recursos

Objetivo Adquirir con oportunidad y calidad técnica los bienes y servicios requeridos por la entidad para su continua operación

Riesgo Identificado Posibilidad de afectación económica por multa o sanción del ente regulador debido a la adquisición de bienes y servicios sin cumplimiento en los requisitos normativos.



Probabilidad Inherente

Moderada 60%

Impacto Inherente

Mayor 80%

Zona de Riesgo

Alta

Fuente: Adaptación propia

Control 1 Cuando se requiera el profesional del área de contratos verifica que la información suministrada por el proveedor corresponda con los requisitos establecidos de contratación a través de una lista de chequeo donde están los requisitos establecidos de información y revisión con la información física suministrada por el proveedor. Los contratos que cumplen son registrados en el sistema de información de contratación. El control está documentado y se guarda evidencia de su ejecución.

Control 2 Cuando se requiera el jefe del área de contratos verifica en el sistema de contratación la información registrada por el profesional asignado y aprueba el proceso para la firma del ordenamiento del gasto en el sistema, en el sistema de contratación queda el registro correspondiente, en caso de encontrar inconsistencias devuelve el proceso al profesional de contratos asignado.

Calificación de los controles Para la calificación de los controles se utiliza la tabla de atributos para evaluar el diseño de los controles, así:

Tabla 16: Aplicación de la tabla de atributos al ejemplo propuesto

Característica			Peso	Control No. 1	Control No. 2
Atributos de eficiencia (65%)	Tipo	Preventivo	20%	20%	-
		Detectivo	10%	-	10%
		Correctivo	5%	-	-
	Implementación	Automático	20%	-	-
		Manual	10%	10%	10%
Atributos informativos	Documentación	Documentado	15%	15%	15%
		Sin documentar	5%	-	-

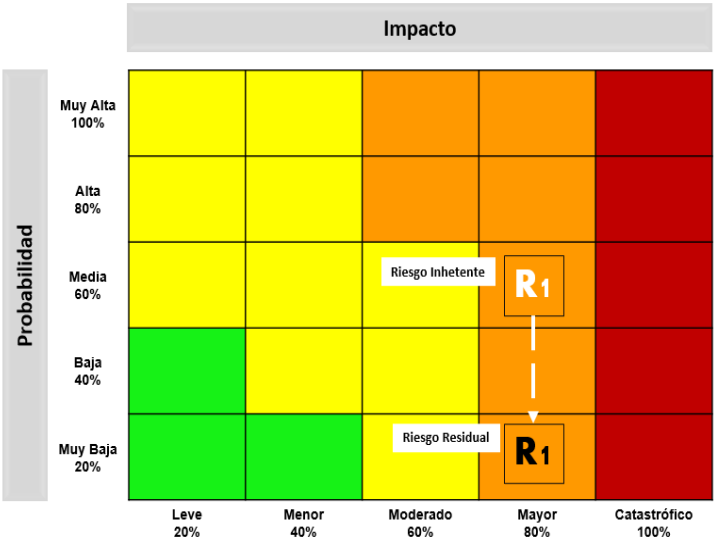
Característica			Peso	Control No. 1	Control No. 2
(35%)	Frecuencia	Continua	10%	10%	10%
		Aleatoria	0%	-	-
	Evidencia	Con registro	5%	5%	5%
		Sin registro	0	-	-
TOTAL				**60%**	**50%**

Fuente: Adaptación propia

Nivel de riesgo residual para riesgos de gestión y seguridad de la información

Para la aplicación de los controles se debe tener en cuenta si este mitiga la probabilidad de ocurrencia o el impacto. Identificado se realizará la reducción uno por uno, como se muestra a continuación.

	Valor Inicial	Valor del Control	Porcentaje para reducir	Reducción Probabilidad
Control No. 1	60%	60%	60% x 60%= **36%**	60% - 36% = **24%**
Control No. 2	24%	50%	24% x 50% = **12%**	24% - 12% = **12%**



Fuente: Adaptación propia

Por probabilidad

12%, es decir que se traslada a la zona muy baja.

Por impacto

El riesgo no tiene controles que ataquen el impacto por los que la valoración permanece igual, mayor 80

Zona de Riesgos Residual

Alta

Análisis y evaluación de controles de corrupción

En virtud que la Guía para la administración del riesgo y el diseño de controles en entidades públicas. Versión 5 de diciembre de 2020, no incluye los lineamientos para el análisis y evaluación de los controles que determinan el riesgo de corrupción residual, se tomará de referencia la Guía para la administración del riesgo y el diseño de controles en entidades públicas. Riesgos de Gestión, Corrupción y Seguridad Digital. Versión 4 octubre de 2018 del Departamento de la Función Pública, así:

Tabla 17: Atributos de calificación de controles para riesgos de corrupción

CRITERIO DE EVALUACIÓN	ASPECTO PARA EVALUAR EN EL DISEÑO DEL CONTROL	OPCIONES DE RESPUESTA	PESO DE LA EVALUACIÓN
RESPONSABLE	¿Existe un responsable asignado a la ejecución del control?	Asignado	15
		No asignado	0
	¿El responsable tiene la autoridad y adecuada segregación de funciones en la ejecución del control?	Adecuado	15
		Inadecuado	0
PERIODICIDAD	¿La oportunidad en que se ejecuta el control ayuda a prevenir la mitigación del riesgo o a detectar la materialización del riesgo de manera oportuna?	Oportuna	15
		Inoportuna	0
PROPÓSITO	¿Las actividades que se desarrollan en el control realmente buscan por si sola prevenir o detectar las causas que pueden dar origen al riesgo?	Prevenir	15
		Detectar	10
		No es control	0
CÓMO SE REALIZA LA ACTIVIDAD DE CONTROL	¿La fuente de información que se utiliza en el desarrollo del control es información confiable que permita mitigar el riego?	Confiable	15
		No confiable	0
QUE PASA CON LAS OBSERVACIONES O DESVIACIONES	¿Las observaciones, desviaciones o diferencias identificadas como resultados de la ejecución del control son investigadas y resueltas de manera oportuna?	Se investigan y resuelven oportunamente	15
		No se investigan y resuelven oportunamente	0
EVIDENCIA DE LA EJECUCIÓN DEL CONTROL	¿Se deja evidencia o rastro de la ejecución del control que permita a cualquier tercero con la evidencia llegar a la misma conclusión?	Completa	10
		Incompleta	5
		No Existe	0

Fuente: Adaptada de la Guía para la administración del riesgo y el diseño de controles en entidades públicas. Riesgos de Gestión, Corrupción y Seguridad Digital. Versión 4 octubre de 2018

Resultados de la evaluación del diseño del control pada riesgos de corrupción

El resultado de cada variable de diseño, a excepción de la evidencia, va a afectar la calificación del diseño del control, ya que deben cumplirse todas las variables para que un control se evalúe como bien diseñado.

Tabla 18: Peso en la evaluación del diseño del control - Riesgos de Corrupción

Rango de calificación del diseño	Resultado: peso en la evaluación del diseño 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 el diseño de controles en entidades públicas. Riesgos de Gestión, Corrupción y Seguridad Digital. Versión 4 octubre de 2018

Si el resultado de las calificaciones del control, o el promedio en el diseño de los controles, está por debajo de 96%, se debe establecer un plan de acción que permita tener un control o controles bien diseñados.

Resultados de la evaluación de la ejecución del control pada riesgos de corrupción

Aunque un control esté bien diseñado, este debe ejecutarse de manera consistente, de tal forma que se pueda mitigar el riesgo. No basta solo con tener controles bien diseñados, debe asegurarse **por parte de la primera línea de defensa** que el control se ejecute. Al momento de determinar si el control se ejecuta, inicialmente, el responsable del proceso debe llevar a cabo una confirmación, posteriormente se confirma con las actividades de evaluación y monitoreo realizadas por la segunda y tercera línea de defensa.

Tabla 19: Peso en la evaluación de la ejecución del control - Riesgos de Corrupción

Rango de calificación del diseño	Resultado: peso en la ejecución del diseño del control
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 el diseño de controles en entidades públicas. Riesgos de Gestión, Corrupción y Seguridad Digital. Versión 4 octubre de 2018

Análisis y evaluación de los controles para la mitigación de los riesgos de corrupción

Dado que la calificación de riesgos inherentes y residuales se efectúa al riesgo y no a

cada causa, hay que consolidar el conjunto de los controles asociados a las causas, para evaluar si estos de manera individual y en conjunto sí ayudan al tratamiento de los riesgos, considerando tanto el diseño, ejecución individual y promedio de los controles. En la evaluación del diseño y ejecución de los controles las dos variables son importantes y significativas en el tratamiento de los riesgos y sus causas, por lo que siempre la calificación de la solidez de cada control asumirá la calificación del diseño o ejecución con menor calificación entre fuerte, moderado y débil, tal como se detalla en la siguiente tabla.

Tabla 20: Determinación de la solidez del control de riesgos de corrupción

Peso del diseño de cada control		Peso de la ejecución de cada control		Solidez individual de cada control		Debe establecer acciones para fortalecer el control
Descripción	Peso	Descripción	Peso	Descripción	Peso	
Fuerte: Calificación entre 96 y 100	96 - 100	**Fuerte:** Siempre se ejecuta	100	fuerte + fuerte = fuerte	Promedio de la suma igual o mayor a 96	No
		Moderado: algunas veces	86	fuerte + Moderado = Moderado	Promedio de la suma inferior a 96	Si
		Débil: no se ejecuta	0	fuerte + débil = Débil	Promedio de la suma inferior a 96	Si
Moderado: Calificación entre 86 y 95	86-95	**Fuerte:** Siempre se ejecuta	100	moderado+ Fuerte = Moderado	Promedio de la suma inferior a 96	Si
		Moderado: algunas veces	86	Moderado + Moderado = Moderado	Promedio de la suma inferior a 96	Si
		Débil: no se ejecuta	0	Moderado + Débil = Débil	Promedio de la suma inferior a 96	Si
Débil: Calificación entre 0 y 85	0 - 85	**Fuerte:** Siempre se ejecuta	100	débil + fuerte = débil	Promedio de la suma inferior a 96	Si
		Moderado: algunas veces	86	débil + moderado = débil	Promedio de la suma inferior a 96	Si
		Débil: no se ejecuta	0	débil + débil = débil	Promedio de la suma inferior a 96	Si

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas. Riesgos de Gestión, Corrupción y Seguridad Digital. Versión 4 octubre de 2018

Nivel de riesgo residual para riesgos de corrupción

Dado que un riesgo puede tener varias causas y varios controles, es necesario evaluar en conjunto los controles asociados al riesgo, de manera que permita determinar el valor del riesgo residual. La solidez del conjunto de controles se obtiene calculando el promedio aritmético simple de los controles por cada riesgo, obteniendo los siguientes resultados:

Tabla 21: Nivel de riesgo residual de corrupción

Rango de calificación del diseño	Calificación de la solidez del conjunto de controles
Fuerte	El promedio de la solidez individual de cada control al sumarlos y ponderarlos es igual a 100
Moderado	El promedio de la solidez individual de cada control al sumarlos y ponderarlos está entre 50 y 99
Débil	El promedio de la solidez individual de cada control al sumarlos y ponderarlos es menor a 50

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas. Riesgos de Gestión, Corrupción y Seguridad Digital. Versión 4 octubre de 2018

Desplazamiento del riesgo inherente para calcular el riesgo de corrupción residual

Dado que ningún riesgo con una medida de tratamiento se evita o elimina, el desplazamiento de un riesgo inherente en su probabilidad para el cálculo del riesgo residual se realizará de acuerdo con la siguiente tabla:

Tabla 22: Desplazamiento del riesgo inherente para calcular el riesgo de corrupción residual

Solidez del conjunto de los controles	Cómo disminuyen la probabilidad	No. De Columnas que se desplazan en el eje de probabilidad
Fuerte	Directamente	2
Fuerte	No disminuye	0
Moderado	Directamente	1
Moderado	No disminuye	0
Débil	No disminuye	0

Fuente: Adaptado de la guía para la administración del riesgo y el diseño de controles en entidades públicas. Riesgos de Gestión, Corrupción y Seguridad Digital. Versión 4 octubre de 2018

6.2.3. Estrategias frente al Riesgo: Tratamiento

El tratamiento del riesgo corresponde a las acciones que se deben tomar, de acuerdo con los lineamientos definidos en la política de Gestión del Riesgo aprobada por la DNBC y que se han sido descrito en este manual. Dichas acciones de tratamiento están encaminadas a las acciones de evitar, reducir y/o aceptar, descritos en las tablas No. 3 Acciones frente al nivel del Riesgo de Gestión y Seguridad de la Información y No. 4 Acciones frente al Riesgo de Corrupción, de acuerdo con el numeral 5.5. Tratamiento del Riesgo.

Ilustración 11: Estrategia del riesgo

Fuente: Imagen propia

- La estratega de aceptación, como su nombre lo indica, se acepta el riesgo como está presente en la entidad, ya que este no genera un impacto significativo a la dirección.

- Las estrategias de reducción están encaminadas a buscar las acciones de mitigación necesarias que permitan minimizar los efectos y/o ocurrencia de los riesgos. Frente a esta estrategia se pueden generar **PLANES DE ACCIÓN**, esto dependerá del diseño y efectividad de las acciones de mitigación implementadas.

- Por último, la estrategia de evitar busca como su nombre lo indica evitar el riesgo por lo tanto se decide no ejecutar las acciones que están asociadas al riesgo, esto se deriva en un cambio de estrategias de operación en la entidad.

Para los riesgos de gestión y seguridad de la información que se identifique inefectivos en las autoevaluaciones realizadas por la primera línea de defensa, monitoreos realizados por la segunda línea de defensa o las evaluaciones realizadas por la tercera línea de defensa, requerirán de planes de acción. Para los riesgos de corrupción aplica lo indicado en la tabla No 19 Determinación de la solidez del control de riesgos de corrupción.

Los planes de acción que se definan para fortalecer y/o implementar medidas de mitigación, pueden estar articulados con la herramienta planes de mejoramiento institucional, definida por el Proceso de Gestión de Análisis y Mejora Continua, donde se consigna los planes establecidos por los procesos para atender los hallazgos y/o observaciones identificadas por Evaluación y Seguimiento en el desarrollo de sus actividades de aseguramiento.

Para aquellos riesgos que requieran en sus planes de acción una inversión adicional a la destinada en el presupuesto del proceso, es necesario que se indique los costos de la inversión y el impacto económico o reputacional de no implementar la medida, de tal manera que el Comité Institucional de Coordinación de Control Interno tome la decisión sobre el caso en particular.

Sobre los planes de acción

El plan de acción no mitiga el riesgo hasta que esté implementado y evaluado por el proceso, una vez eso suceda, el proceso debe reportar al proceso de Gestión de Análisis y Mejora Continua el plan de acción como terminado con el fin de verificar con el proceso y de ser necesario establecer el control que resulta del plan de acción y ajustar la valoración del respectivo riesgo.

El plan de acción como mínimo debe contener los siguientes campos:

Tabla 23: Elementos mínimos el diseño del plan de acción

Elemento	Descripción
Fecha de diseño	Es la fecha en la que se propone la acción a realizar por parte del proceso.
Objetivo del Plan de acción	Responde al propósito que el plan de acción tiene, por lo general responderá a dar respuesta a una causa raíz del riesgo.
Detalle de las actividades	Describe las acciones que se van a ejecutar y puede ser más de una actividad para lograr el plan de acción. Por ejemplo, si el plan de acción corresponde a la implementación de un proceso, este tendrá actividades de diseño, validación y aprobación.
Responsables	Por acción se debe reportar quien es el responsable de su ejecución.
Fecha de implementación	Por actividad se debe reportar la fecha de implementación, llegando a la fecha final en la que el plan de acción esté listo para ser puesto a ejecución.
Costos	Si el plan de acción requiere de una inversión económica debe indicarse, igualmente si el proceso cuenta con ese presupuesto o debe ser solicitado al Comité Institucional de Coordinación de Control Interno.

Fuente: Adaptación Propia

Si alguno de los atributos cambia deben ser reportados al proceso de Gestión de Análisis y Mejora Continua junto con la justificación respectiva, quien reportará los avances al Comité Institucional de Coordinación de Control Interno.

Una vez el plan de acción entre a ejecución, el Líder del Proceso junto con el Gestor respectivo deben evaluar si el plan de acción tuvo los resultados esperados, lo cual debe realizarse dentro de los tres primeros meses de haberse implementado el plan de acción y notificad o al proceso de Gestión de Análisis y Mejora Continua para realizar el ajuste a la matriz de riesgos del proceso.

6.2.4. Herramientas para la gestión del riesgo

Producto de la aplicación de la metodología se desarrollarán mapas de riesgo, además se definirán registros y reportes necesarios para su monitoreo, que permita la mejora continua de la entidad. Al respecto la DNBC define los siguientes.

Reporte de eventos

El evento es un riesgo materializado, es decir corresponden a situaciones que durante el día a día de los procesos se puede presentar, generando alguna pérdida económica o reputacional. Dichos eventos pueden estar asociados a riesgos que no estuvieron identificados por los procesos, por lo que se hace necesario reportarlos. El reporte de evento permite:

- Mantener una base histórica de eventos que permita diseñar estrategias adecuadas para que a futuro no se repitan.
- Analizar si el evento se presenta por un error en la formulación, ejecución o ausencia de controles.
- Actualizar las matrices de riesgos ajustándolas a la realidad de la operación del proceso.
- Mejorar el Sistema de Gestión del Riesgo.

Todos los funcionarios y contratistas de la entidad podrán reportar al proceso de Gestión de Análisis y Mejora Continua cualquier situación que considere que ha generado un evento de riesgos, para lo cual se debe seguir el paso a paso que se defina en el instructivo de reporte de eventos.

Otras fuentes de información que el profesional de Planeación analizará para el reporte de eventos son:

- Mesas de ayuda
- PQRD (Peticiones, quejas, reclamos, denuncias)
- Reporte de las posibles contingencias de la DNBC
- Líneas internas de denuncia
- Reportes de Control Interno

Procedimiento para el análisis de eventos

a. Mensualmente revisará el reporte de eventos y de encontrar registros procederá a realizar investigación de los hechos reportados. Las otras fuentes de información serán revisadas de manera trimestral.

b. Si como resultado se identifica que el evento corresponde a la materialización de un riesgo (identificado o no) se solicita reunión con el proceso para verificar la situación.

c. Se ajusta la valoración del riesgo y el control. Así mismo se diseñará o modificará los planes de acción definidos por el proceso para atender la situación evidenciada.

d. El gestor del proceso realiza seguimiento a las acciones definidas y reporta al proceso de Gestión de Análisis y Mejora Continua, junto con los otros planes de acción, según lo definido en el numeral 6.2.4. tratamiento.

e. El proceso de Gestión de Análisis y Mejora Continua reportará los eventos de riesgos junto con las acciones realizadas con los procesos, por lo menos una vez cada seis meses.

f. En el caso que, el evento presentado genera un impacto alto o externos para la entidad el proceso de Evaluación y Seguimiento reportará al Comité de Coordinación de Control Interno de manera inmediata.

Indicadores clave de riesgos

Hace referencia a una colección de datos históricos, por periodos de tiempo, relacionados con algún evento cuyo comportamiento puede indicar una mayor o menor exposición a determinados riesgos. No indica materialización de los riesgos, pero sugiere que algo no funciona adecuadamente y, por lo tanto, se debe investigar.

Los indicadores claves de riesgo o KRI (Key Risk Indicator), permite capturar la ocurrencia de un incidente que se asocia a un riesgo identificado previamente y que es considerado alto, lo cual permite llevar un registro de ocurrencias y evaluar a través de su tendencia la eficacia de los controles que se disponen para mitigarlos, algunos ejemplos son:

Tabla 24: Ejemplos de Indicadores de Riesgos

Proceso Asociado	Indicador	Métrica
TIC	Tiempo de interrupción de aplicativos críticos en el mes	Número de horas de interrupción de aplicativos críticos del mes
Financiera	Reportes emitidos al regulador fuera del tiempo establecido	Número de reportes mensuales remitidos fuera de los términos
Atención al Usuario	Reclamos de usuario por incumplimiento a términos de ley o reiteraciones de solicitudes por conceptos no adecuados	% de solicitudes mensuales fuera de términos % de solicitudes reiteradas por tema
Administrativo y Financiera	Errores den transacciones y su impacto en la gestión presupuestal	Volumen de transacciones al mes sobre la capacidad disponible
Talento Humano	Rotación de personal	% de nuevos empleados que abandonan el puesto dentro de los primeros 6 meses.

Fuente: Tomado de la Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 5

La Dirección nacional de Bomberos de Colombia definirá KRI a los riesgos de calificación "alta" y "extrema" que afectan la misionalidad de la entidad. Dichos indicadores serán construidos una vez se implemente la versión 2 del Manual de Gestión del Riesgo y serán monitoreados de manera cuatrimestral, así mismo por lo menos una vez al año se revisará el mapa de indicadores definidos y de requerirse serán actualizados.

6.2.5. Monitoreo y revisión

Los resultados de monitoreo y la revisión se deben registrar y reportar interna y externamente según corresponda y deben utilizarse como una entrada para la revisión de la política y procedimientos de la Gestión del Riesgo.

Cada una de las líneas de defensa tiene un rol sobre el monitoreo y reporte que debe mantenerse en la Gestión del Riesgo de la DNBC y que a continuación se menciona.

Línea Estratégica

Es responsable de hacer el seguimiento de los riesgos que se encuentren en calificación residual "alta" y "extrema", así como de los reportes que emita la segunda y tercera línea de defensa sobre la Gestión del Riesgo. Las decisiones y conclusiones que tome esta línea deben documentarse para que se haga el adecuado seguimiento.

Primera Línea de Defensa

Mediante el autocontrol los Líderes de Proceso junto con sus Gestores deben realizar el seguimiento de sus riesgos, controles y planes de acción definidos, en particular frente a la Gestión del Riesgo debe:

- Reportar y facilitar las evidencias en el monitoreo de los riesgos cuando sea requerido por el proceso de Gestión de Análisis y Mejora Continua y/o el proceso de Evaluación y Seguimiento.
- Monitorear periódicamente sus riesgos, garantizando la eficiencia, eficacia y efectividad de las acciones de tratamiento y reportar de manera cuatrimestral sus resultados al proceso de Gestión de Análisis y Mejora Continua.
- Construir y enviar al proceso de Gestión de Análisis y Mejora Continua el informe de monitoreo cuatrimestral de los riesgos de corrupción.
- Hacer seguimiento a los planes de acción definidos para mitigar sus riesgos y reportar al proceso de Gestión de Análisis y Mejora Continua su implementación.

Segunda Línea de Defensa

Su rol principal es el monitoreo de la Gestión del Riesgo ejecutada por la primera línea de defensa, por lo que debe:

- Hacer seguimiento de los reportes de eventos e indicadores claves de riesgos. Resultado de ese seguimiento el proceso de Gestión de Análisis y Mejora Continua podrá solicitar ajustes de las matrices de riesgos a los procesos.

- Consolidar las evidencias de la ejecución de las medidas de tratamiento definidas por los procesos, así como el avance de los planes de acción de los riesgos de corrupción, solicitar los ajustes, definir acciones de mejoramiento y reportar al proceso de Evaluación y Seguimiento los resultados.
- Analizar los reportes de autoevaluación entregados por la primera línea de defensa.
- Definir un plan de monitoreo de las matrices de riesgos a revisar durante el año y solicitar al proceso los ajustes que sean necesarios.
- Reportar semestralmente al Comité Interno de Coordinación de Control Interno los resultados del monitoreo de la Gestión del Riesgo.
- Cuando se materialice un riesgo de nivel "alto" o "extremo" se deberá reportar de manera inmediata al Comité Interno de Coordinación de Control Interno para que dicho órgano defina las estrategias necesarias para subsanar la situación.

Tercera Línea de Defensa

Mediante el aseguramiento a través de sus actividades de auditoría interna, la tercera línea de defensa es responsable de:

- Evaluar la efectividad y la aplicación de controles, planes de contingencia y actividades de monitoreo vinculadas a los cambios que pueden afectar el Sistema de Control Interno para el cumplimiento de los objetivos.
- Construir y enviar a la Alta Dirección el informe de monitoreo cuatrimestral de los riesgos de corrupción.
- Construir y enviar a la Alta Dirección el informe de monitoreo de los riesgos de gestión y seguridad de la información, según programación del Plan Anual del Auditoría - PAA.

6.2.6. Comunicación y Consulta

La comunicación y consulta busca la participación de las partes interesadas, tanto internas como externas, durante todas las etapas de la Gestión del Riesgo. Por lo que la comunicación entre las líneas de defensa con los funcionarios y contratistas es esencial mediante los diferentes canales de comunicación que tiene la entidad, principalmente se define.

- El mapa de Riesgos de la DNBC estará publicado en el enlace compartido en línea de la DNBC para consulta de todos los funcionarios y contratistas.
- Todos los funcionarios y contratistas podrán revisar y retroalimentar en términos de aportar su conocimiento en la identificación, análisis y valoración del riesgo, así como en la ejecución de las acciones definidas para el tratamiento de los riesgos.
- Los líderes de los procesos y sus gestores son responsables de divulgar y sensibilizar al interior de sus procesos el mapa de riesgos junto con el plan de acción definido.
- El proceso de Gestión de Análisis y Mejora Continua impulsará a nivel institucional una cultura de Gestión del Riesgo, a través de capacitaciones, mesas de trabajo y asesorías, con el fin de mejorar el conocimiento y apropiación del enfoque basado en riesgos.
- El proceso de Gestión de Análisis y Mejora Continua realiza la consolidación de los Mapas

de Riesgos.

- La consulta y divulgación del Mapa de Riesgos a partes interesadas y comunidad en general se realiza a través de su publicación en la página web de la DNBC.
- El proceso de Evaluación y Seguimiento publicará los resultados de los seguimientos a los mapas de riesgos en la página web de la DNBC.

Sobre el manejo de los mapas de riesgo

Los líderes de los procesos son responsables de la actualización de sus mapas de riesgos, los cuales están publicadas en el enlace compartido en línea de la DNBC para su permanente consulta, no obstante, los procesos solo tendrán la opción de lectura del documento, esto con el fin para mitigar cualquier riesgo de integridad y calidad de la información. Los ajustes que solicite el proceso serán realizados por el proceso de Gestión de Análisis y Mejora Continua, quienes serán los únicos quien tendrán la opción de editar el documento.

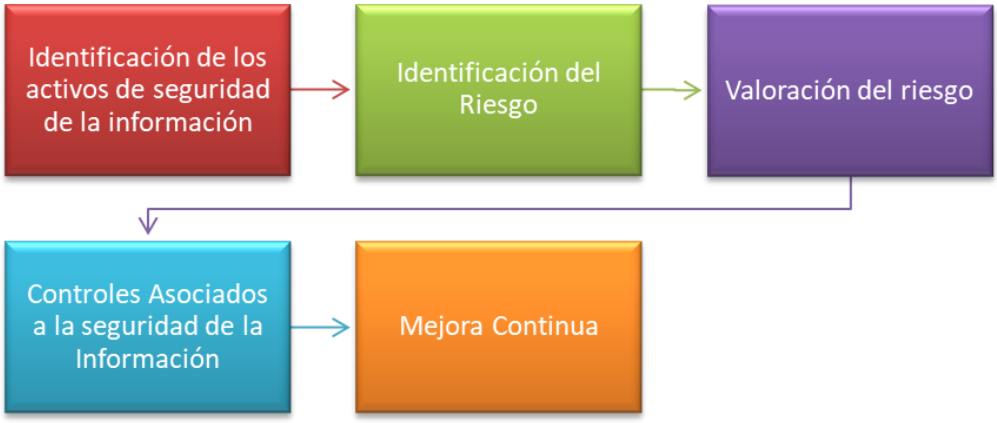
Capacitaciones de la Gestión del Riesgo

El proceso de Gestión de Análisis y Mejora Continua prepara el plan de capacitaciones anual sobre los temas específicos de Riesgos de Gestión y de Corrupción, en el cual se dará a conocer los resultados del monitoreo de la Gestión del Riesgo de la DNBC y las nuevas estrategias para su fortalecimiento, por lo que su contenido será revisado anualmente.

Además, participa en las capacitaciones de inducción con los contenidos relevantes de la Gestión del Riesgos de la entidad.

7. RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Ilustración 12: Metodología de la Gestión de Riesgos de Seguridad de la Información



Fuente: Elaboración propia adaptado de la Resolución 00500 de 2021

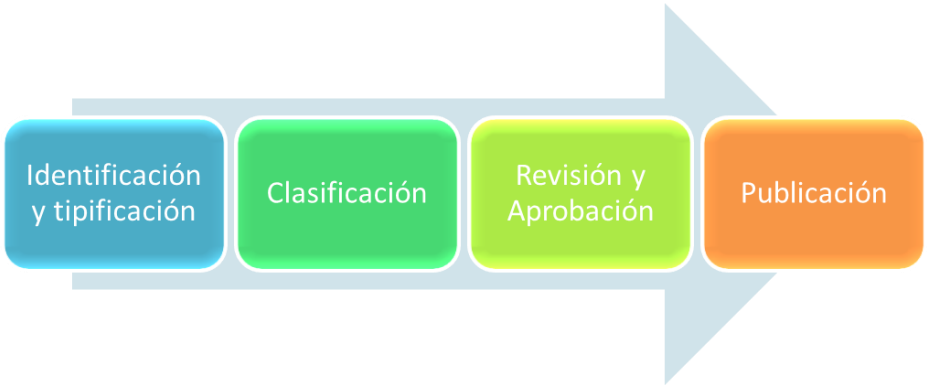
Una vez la Dirección Nacional de Bomberos de Colombia defina las políticas y procedimientos para la implementación del Modelo de Seguridad y Privacidad de la Información – MSPI, los Riesgos de Seguridad de la Información se articularán con dicho modelo. La metodología para

la valoración de los riesgos y seguridad de la información se presenta a continuación.

7.1. Identificación de los activos de seguridad de la información

Con el fin de efectuar una adecuada identificación de los riesgos asociados a la seguridad de la información se hace necesario realizar un inventario y clasificación de los activos que hacen parte de las actividades más relevantes e importantes del Modelo de Seguridad y Privacidad de la Información, para ello se llevan a cabo las siguientes fases:

Ilustración 13: Pasos para la identificación de activos de seguridad de la información



Fuente: Elaboración propia adaptado de la Resolución 00500 de 2021

7.1.1. Identificación y tipificación de los activos de información

El proceso como propietario y custodio de la información que produce debe identificar, clasificar y valorar los activos de información, teniendo en cuenta:

d. Lo establecido en la norma técnica ISO/IEC 27000: Información; Software como programa informático; Hardware como computadora; servicios; personas, y sus calificaciones, habilidades y experiencia; intangibles como reputación e imagen.

e. Las Tablas de Retención Documental actualizadas de la DNBC, que contemplan las series, subseries tipos documentales de la información producida, así como su medio de conservación y preservación. Las fuentes de información no contempladas en este documento, deben ser identificadas por los gestores, con el Líder del proceso.

   La información básica hace referencia a aquellas características mínimas del activo que debe identificarse durante esta fase y que son:

   - Identificador: Número consecutivo único que identifica al activo en el inventario.
   - Proceso: Nombre del proceso al que pertenece el activo.
   - Nombre Activo: Nombre de identificación del activo dentro del proceso al que pertenece.
   - Descripción/Observaciones: Es un espacio para describir el activo de manera que sea claramente identificable por todos los miembros del proceso.
   - Ubicación: Describe la ubicación tanto física como electrónica del activo de información.

- Propietario: Es una parte designada de la entidad, un cargo, proceso, o grupo de trabajo que tiene la responsabilidad de garantizar que la información y los activos asociados con el proceso se clasifican adecuadamente. Deben definir y revisar periódicamente las restricciones y clasificaciones del acceso.
- Custodio: Es una parte designada de la entidad, un cargo, proceso, o grupo de trabajo encargado de hacer efectivos las restricciones y clasificaciones de acceso definidos por el propietario.
- Tipo: Define el tipo al cual pertenece el activo. Para este campo se utilizan los siguientes valores:

Tabla 25: Tipificación de activos

TIPIFICACIÓN DEL ACTIVO	DESCRIPCIÓN	COMPONENTES
Información	Corresponden a este tipo de datos e información almacenada o procesada electrónicamente tales como: • Bases y archivos de datos • Contratos, documentación del sistema • Investigaciones • Acuerdos de confidencialidad • Manuales de usuario • Procedimientos operativos o soporte • Planes para la continuidad del negocio • Acuerdos sobre el retiro • Pruebas de auditoría, • entre otros.	
Hardware	Se consideran los medios materiales físicos destinados a soportar directa o indirectamente los servicios que presta la entidad	• Servidores • Routers • Módems • Computadores (portátiles y de escritorio) • Celulares • Tablet, Teléfonos IP
Software	Se refiere a los programas, aplicativos, sistemas de información que soportan las actividades de la entidad y la prestación de los servicios.	Software de aplicación, correo electrónico, sistema operativo, etc
Servicios	Servicios de computación y comunicaciones, tales como Internet, páginas de consulta, directorios compartidos e Intranet.	

TIPIFICACIÓN DEL ACTIVO	DESCRIPCIÓN	COMPONENTES
Recurso Humano	Aquellas personas que, por su conocimiento, experiencia y criticidad para el proceso, son consideradas activos de información.	Contratistas, funcionarios, proveedores
Instalaciones	Lugares donde se almacena o resguardan los sistemas de información y comunicaciones.	Centros de cómputo, centros de cableado, Datacenter.
Infraestructura crítica cibernética nacional	Se entiende por aquella infraestructura soportada por las TIC y por las tecnologías de operación, cuyo funcionamiento es indispensable para la prestación de servicios esenciales para los ciudadanos y para el Estado. Su afectación, suspensión o destrucción puede generar consecuencias negativas en el bienestar económico de los ciudadanos, o en el eficaz funcionamiento de las organizaciones e instituciones, así como de la administración pública.	

Fuente: Anexo 1 de la Resolución 00500 de marzo de 2021 emitida por el Ministerio de Tecnologías de la Información y las Comunicaciones, MINTIC

Con el fin de mantener una tipificación de activos actualizada, de manera anual la DNBC realizará un inventario a los activos de seguridad de la información, no obstante, sin antes que se realice el inventario periódico se identifica alguna situación que genera un cambio como: la adquisición o inclusión de un nuevo activo, ajuste a un proceso o procedimiento, movimientos físicos de archivos, migraciones de información, entre otros, se deberá registra de manera inmediata en el inventario.

7.1.2. Clasificación de activos de información

La clasificación de activos de información tiene como objetivo asegurar que la información recibe los niveles de protección adecuados de acuerdo con sus características particulares, se basa en la Confidencialidad, la Integridad y la Disponibilidad de cada activo, asimismo, contempla el impacto que causaría la pérdida de alguna de estas propiedades.

Cada activo identificado será clasificado para establecer el criterio específico y lineamiento para su adecuado tratamiento. La DNBC adopta los lineamientos definidos en la Resolución 00500 de marzo de 2021 del Ministerio de las Tecnologías – MINTIC, que se describen a continuación:

Tabla 26:Criterios de Clasificación

CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
INFORMACIÓN PÚBLICA RESERVADA	ALTA (A)	ALTA (A)
INFORMACIÓN PÚBLICA CLASIFICADA	MEDIA (M)	MEDIA (M)
INFORMACIÓN PÚBLICA	BAJA (B)	BAJA (B)
NO CLASIFICADA	NO CLASIFICADA	NO CLASIFICADA

Fuente: Anexo 1 de la Resolución 00500 de marzo de 2021 emitida por el Ministerio de Tecnologías de la Información y las Comunicaciones, MINTIC

Para realizar una adecuada clasificación de los activos se describe cada uno de los criterios:

Confidencialidad

La confidencialidad se refiere a que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados, esta se debe definir de acuerdo con las características de los activos que se manejan en cada entidad, la DNBC adopta los (3) niveles definidos en el Anexo 1 de la Resolución 00500 de marzo de 2021 de MINTIC, que están alineados con los tipos de información declarados en la ley 1712 del 2014.

Tabla 27: Descripción del Criterio de Confidencialidad

CRITERIO	DESCRIPCIÓN
INFORMACIÓN PÚBLICA RESERVADA	Información disponible sólo para un proceso de la entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo de índole legal, operativa, de pérdida de imagen o económica
INFORMACIÓN PÚBLICA CLASIFICADA	Información disponible para todos los procesos de la entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo para los procesos de la misma. Esta información es propia de la entidad o de terceros y puede ser utilizada por todos los funcionarios de la entidad para realizar labores propias de los procesos, pero no puede ser conocida por terceros sin autorización del propietario.
INFORMACIÓN	Información que puede ser entregada o publicada sin

CRITERIO	DESCRIPCIÓN
PÚBLICA	restricciones a cualquier persona dentro y fuera de la entidad, sin que esto implique daños a terceros ni a las actividades y procesos de la entidad.
NO CLASIFICADA	Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de INFORMACIÓN PUBLICA RESERVADA.

Fuente: Anexo 1 de la Resolución 00500 de marzo de 2021 emitida por el Ministerio de Tecnologías de la Información y las Comunicaciones, MINTIC

Integridad

La integridad se refiere a la exactitud y completitud de la información (ISO 27000) esta propiedad es la que permite que la información sea precisa, coherente y completa desde su creación hasta su destrucción. La DNBC adopta los (3) niveles definidos en el Anexo 1 de la Resolución 00500 de marzo de 2021 de MINTIC.

Tabla 28:Descripción del Criterio de Integridad

CRITERIO	DESCRIPCIÓN
ALTA (A)	Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas de la entidad.
MEDIA (M)	Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen moderado a funcionarios de la entidad.
BAJA (B)	Información cuya pérdida de exactitud y completitud conlleva un impacto no significativo para la entidad o entes externos.
NO CLASIFICADA	Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de información de integridad ALTA.

Fuente: Anexo 1 de la Resolución 00500 de marzo de 2021 emitida por el Ministerio de Tecnologías de la Información y las Comunicaciones, MINTIC

Disponibilidad

La disponibilidad se refiere a la información que debe ser accesible y utilizable por solicitud de una persona, entidad o proceso autorizada cuando así lo requiera en el momento y en la forma, al igual que los recursos necesarios para su uso. La DNBC adopta los (3) niveles definidos en el Anexo 1 de la Resolución 00500 de marzo de 2021 de MINTIC.

Tabla 29: Descripción del Criterio de Disponibilidad

CRITERIO	DESCRIPCIÓN
ALTA (A)	La no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas a entes externos.
MEDIA (M)	La no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen moderado de la entidad.
BAJA (B)	La no disponibilidad de la información puede afectar la operación normal de la entidad o entes externos, pero no conlleva implicaciones legales, económicas o de pérdida de imagen.
NO CLASIFICADA	Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de información de disponibilidad ALTA

Fuente: Anexo 1 de la Resolución 00500 de marzo de 2021 emitida por el Ministerio de Tecnologías de la Información y las Comunicaciones, MINTIC

Niveles de clasificación

Teniendo en cuenta las anteriores clasificaciones la DNBC determinara el nivel de criticidad del activo, teniendo en consideración la siguiente tabla definida en el Anexo 1 de la Resolución 00500 de marzo de 2021 de MINTIC, que adopta DNBC.

Tabla 30: Niveles de Clasificación

NIVEL	DESCRIPCIÓN
ALTO	Activos de información en los cuales la clasificación de la información en dos (2) o todas las propiedades (confidencialidad, integridad, y disponibilidad) es alta.
MEDIO	Activos de información en los cuales la clasificación de la información es alta en una (1) de sus propiedades o al menos una de ellas es de nivel medio.
BAJO	Activos de información en los cuales la clasificación de la información en todos sus niveles es baja.

Fuente: Anexo 1 de la Resolución 00500 de marzo de 2021 emitida por el Ministerio de Tecnologías de la Información y las Comunicaciones, MINTIC

La DNBC gestionará los riesgos de los activos del inventario que tengan un nivel de criticidad Alto según lo dispuesto en la política.

Revisión, aprobación y publicación de los activos de la información

El proceso para la revisión, aprobación y publicación de los activos de la información de la DNBC deberá hacerse por parte del responsable de la política en el Modelo se Seguridad y Privacidad de la Información – MSPI por lo menos una vez al año.

7.2. Identificación del riesgo

Para los activos que se gestionen, se podrán identificar los siguientes tres (3) riesgos inherentes de seguridad de la información:

- Pérdida de la confidencialidad
- Pérdida de la integridad
- Pérdida de la disponibilidad

Para cada riesgo se deben asociar al grupo de activos, o activos específicos del proceso, y conjuntamente analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización.

A continuación, se mencionan un listado de amenazas y vulnerabilidades que podrían materializar los tres (3) riesgos previamente mencionados:

Identificación de Amenazas: Se plantean los siguientes listados de amenazas, que representan situaciones o fuentes que pueden hacer daño a los activos y materializar los riesgos. A manera de ejemplo se citan las siguientes amenazas: Deliberadas (D), fortuito (F) o ambientales (A)

Tabla 31: Tabla de Amenazas Comunes

Tipo	Amenazas	Origen
Daño físico	Fuego	F, D, A
	Agua	F, D, A
Eventos naturales	Fenómenos climáticos	A
	Fenómenos sísmicos	A
Pérdidas de los servicios esenciales	Fallas en el sistema de suministro de agua	A
	Fallas en el suministro de aire acondicionado	F, D, A
Perturbación debida a la radiación	Radiación electromagnética	F, D, A
	Radiación térmica	F, D, A
Compromiso de la información	Interceptación de servicios de señales de interferencia comprometida	D
	Espionaje remoto	D
	Fallas técnicas Fallas del equipo	D, F
	Mal funcionamiento del equipo	D, F

Tipo	Amenazas	Origen
	Saturación del sistema de información	D, F
	Mal funcionamiento del software	D, F
	Incumplimiento en el mantenimiento del sistema de información	D, F
Acciones no autorizadas	Uso no autorizado del equipo	D, F
	Copia fraudulenta del software	D, F
Compromiso de las funciones	Error en el uso o abuso de derechos	D, F
	Falsificación de derechos	D

Fuente: ISO 27005:2009

Amenazas dirigidas por el hombre: empleados con o sin intención, proveedores y piratas informáticos, entre otros.

Fuente de Amenaza	Motivación	Acciones Amenazantes
Pirata informático, intruso ilegal	Reto Ego	Piratería Ingeniería social
Criminal de la computación	Destrucción de la información Divulgación ilegal de la información	Crimen por computador Acto fraudulento
Terrorismo	Chantaje Destrucción	Ataques contra el sistema DDoS Penetración en el sistema
Espionaje industrial (inteligencia, empresas, gobiernos extranjeros, otros intereses)	Ventaja competitiva Espionaje económico	Ventaja de defensa Hurto de información
Intrusos (empleados con entrenamiento deficiente, descontentos, malintencionados, negligentes, deshonestos o despedidos)	Curiosidad Ganancia monetaria	Asalto a un empleado Chantaje

Fuente: ISO/IEC 27005:2009

Identificación de vulnerabilidades: la entidad pública puede identificar vulnerabilidades (debilidades).

Tipo	Vulnerabilidades
Hardware	• Mantenimiento insuficiente • Ausencia de esquemas de reemplazo periódico • Sensibilidad a la radiación electromagnética • Susceptibilidad a las variaciones de temperatura (o al polvo y suciedad) • Almacenamiento sin protección Falta de cuidado en la disposición final Copia no controlada
Software	• Ausencia o insuficiencia de pruebas de software • Ausencia de terminación de sesión • Ausencia de registros de auditoría • Asignación errada de los derechos de acceso • Interfaz de usuario compleja • Ausencia de documentación • Fechas incorrectas • Ausencia de mecanismos de identificación y autenticación de usuarios • Contraseñas sin protección • Software nuevo o inmaduro
Red	• Ausencia de pruebas de envío o recepción de mensajes • Líneas de comunicación sin protección • Conexión deficiente de cableado • Tráfico sensible sin protección • Punto único de falla
Personal	• Ausencia del personal • Entrenamiento insuficiente • Falta de conciencia en seguridad • Ausencia de políticas de uso aceptable • Trabajo no supervisado de personal externo o de limpieza
Lugar	• Uso inadecuado de los controles de acceso al edificio • Áreas susceptibles a inundación • Red eléctrica inestable • Ausencia de protección en puertas o ventanas
Organización	• Ausencia de procedimiento de registro/retiro de usuarios • Ausencia de proceso para supervisión de derechos de acceso • Ausencia de control de los activos que se encuentran fuera de las instalaciones • Ausencia de acuerdos de nivel de servicio (ANS o SLA) • Ausencia de mecanismos de monitoreo para brechas en la

Tipo	Vulnerabilidades
	seguridad • Ausencia de procedimientos y/o de políticas en general (esto aplica para muchas actividades que la entidad no tenga documentadas y formalizadas como uso aceptable de activos, control de cambios, valoración de riesgos, escritorio y pantalla limpia entre otros)

Fuente: ISO/IEC 27005

La sola presencia de una vulnerabilidad no causa daños por sí misma, ya que representa únicamente una debilidad de un activo o un control, para que la vulnerabilidad pueda causar daño, es necesario que una amenaza pueda explotar esa debilidad. Una vulnerabilidad que no tiene una amenaza puede no requerir la implementación de un control.

Ejemplo

Tabla 32: Correlación de amenazas y vulnerabilidades de acuerdo con el tipo de activo

Tipo de Activo	Ejemplo de vulnerabilidades	Ejemplo de Amenazas
Hardware	Almacenamiento de medios sin protección	Hurto de medios o documentos
Software	Ausencia de parches de seguridad	Abuso de los derechos
Red	Líneas de comunicaciones sin protección	Escucha encubierta
Información	Falta de controles de acceso físico	Hurto de Información
Personal	Falta de capacitación en las herramientas	Error en el Uso
Organización	Ausencia de Política de Seguridad	Abuso de derechos

Fuente: Ministerio de Tecnologías de la Información y Comunicaciones MINTIC, 2018

7.3. Valoración del riesgo de seguridad de la información

Para la valoración del riesgo de Seguridad de la Información se asociarán las tablas de probabilidad e impacto aprobadas por la Línea Estratégica y que se encuentran detalladas en el capítulo 4 de este manual.

7.4. Controles asociados a la seguridad de la información

El control que mitiga o reduce el riesgo debe ser identificado y valorado teniendo en cuenta las características descritas en el numeral 6.2.2. Evaluación del riesgo, para el caso particular de Seguridad de la Información existen algunos controles previamente definidos en el Anexo A de la ISO/IEC 27001:2013 que se describen en el anexo 4 del "Modelo Nacional de Gestión del Riesgo de Seguridad de la Información en entidades públicas" lo cuales podrán ser adoptados por la DNBC ajustando sus características al diseño y ejecución de la operación normal de la entidad.

7.5. Mejora continua

Cuando existan hallazgos, falencias o incidentes de seguridad digital se debe:

- Mitigar el impacto de su existencia y tomar acciones para controlarlos y prevenirlos.
- Establecer y hacer frente a las consecuencias propias de la no conformidad que llegó a materializarse.
- Definir las acciones para mejorar continuamente la Gestión del Riesgos de seguridad digital de la siguiente forma:
  - ✓ Revisar y evaluar los hallazgos encontrados en las auditorías internas, otras auditorías e informes de los entes de control realizadas.
  - ✓ Establecer las posibles causas y consecuencias del hallazgo.
  - ✓ Determinar si existen otros hallazgos similares para establecer acciones correctivas y evitar así que se lleguen a materializar.
  - ✓ Emprender acciones de revisión continua, que permitan gestionar el riesgo a tiempo, disminuir el impacto y la probabilidad de ocurrencia del riesgo detectado, así como la aparición de nuevos riesgos que puedan afectar el desempeño de la DNBC o de los servicios que presta al ciudadano.
  - ✓ Llevar un registro documentado del tratamiento realizado al hallazgo, así como las acciones realizadas para mitigar el impacto y ver el resultado para futuros hallazgos.

8. CONTROL DE CAMBIOS

FECHA	CAMBIO	VERSIÓN
22/10/2019	Documento Nuevo – Reemplaza la Guía Análisis y Mejora Continua	**1**
30/06/2021	Se adapta la Guía de Gestión del Riesgo a la nueva versión de la Guía para la administración del riesgo y el diseño de controles en entidades públicas emitida por la Dirección de Gestión y Desempeño Institucional de diciembre de 2020. Los principales cambios están: • Redacción del riesgo identificado. • Definición de nuevas tablas de impacto y probabilidad para la valoración del riesgo. • Implementación de los lineamientos de los riesgos de seguridad de la información.	**2**
31/01/2021	Se incluye las recomendaciones realizadas por el la Oficina de Control Interno en cuanto: • Nota aclaratoria sobre las partes interesadas de la DNBC para la valoración del impacto reputacional. • Ajuste tabla No. 6 Factores de Riesgos • Ajuste tabla No. 7 Elementos descriptivos del riesgo • Ajuste tabla No. 8 Clasificación de riesgos de la DNBC • Ajuste tabla No. 12 Ejemplo de la redacción de un control • Ajuste del numeral 6.1.4. Identificación de riesgos de gestión y corrupción, incluyendo aclaraciones sobre la identificación del riesgo de corrupción.	**3**
4/11/2022	• Se incluyen en las definiciones conceptos claves para el manejo de los riesgos de seguridad de la información. • Se realiza ajuste en la medición del riesgo residual para los riesgos de	**4**

	corrupción, de conformidad a la Guía de orientación de aplicación del Modelo Nacional de Gestión de Riesgos de Seguridad Digital - GRSD en el sector público, territoriales y gobierno nacional. 2018 • Se ajusta el numeral 5.5. Tratamiento del riesgo, articulando las acciones de monitoreo y la definición de planes de acción.	

Elaborado por:	Revisado y Aprobado por:	Revisión metodológica:
Nombre: Merle Johana Galindo Olaya **Cargo:** Profesional Gestión de Análisis y Mejora Continua **Fecha:** 4/11/2022 **Firma:**	**Nombre:** Comité Institucional de Coordinación de Control Interno **Cargo:** Comité **Fecha:** 4/11/2022 **Firma:**	**Nombre:** Adriana Moreno / John Jairo Beltrán **Cargo:** Profesional con funciones de Planeación / Contratista Gestión de Análisis y Mejora Continua **Fecha:** 4/11/2022 **Firma:**