Metodología de Administración de Riesgos

UNIDAD PARA LAS VÍCTIMAS

TODOS POR UN NUEVO PAÍS
PAZ EQUIDAD EDUCACIÓN

TABLA DE CONTENIDO

2. INTRODUCCIÓN

La Unidad a partir de agosto de 2013 diseñó e implementó el componente de Administración de Riesgos, fortalecer al Sistema de Control Interno de la Unidad, aplicando una metodología semicuantitativa con el fin de identificar y valorar los riesgos en las actividades o eventos que puedan afectar de forma negativa el cumplimiento de la misión, visión, objetivos institucionales, metas, proyectos de la Unidad para las Víctimas, entre otros; esto permite el fortalecimiento de la cultura del autocontrol y autoevaluación y la identificación de acciones y oportunidades para el mejoramiento continuo y optimización de la gestión institucional.

A partir del 2017, la Unidad pretende integrar a esta metodología los riesgos públicos (de seguridad de las personas), seguridad de la información y seguridad y salud en el trabajo, con el fin de gestionar los riegos a los cuales la Entidad se encuentra expuesta de manera integral.

3. OBJETIVO

Establecer la Metodología de Administración de Riesgos Integrales de la Unidad con el fin de identificar, valorar y dar tratamiento a los riesgos institucionales de la Unidad.

4. DEFINICIONES

Actividad: Agrupación de tareas que hace parte de un Proceso.

Autocontrol: Capacidad de controlarse uno mismo.

Calificación de Riesgos: cuantificación de los riesgos de acuerdo con la probabilidad de ocurrencia o frecuencia y sus consecuencias.

Componente: Agrupación de elementos que hace parte de un subsistema.

Control: los controles son acciones o actividades que deben apuntar a mitigar las causas generadoras del riesgo.

Efectividad de los controles: medida de lo apropiado de un control, establecida bajo dos parámetros: su eficiencia y eficacia.

Efecto: consecuencia que puede traer la ocurrencia del riesgo.

Eficacia de los controles: medida de lo apropiado de un control establecida al determinar su contribución con el objetivo del mismo, es decir, con la disminución del riesgo.

Eficiencia de los controles: medida del uso adecuado de los recursos en la aplicación de un control.

Elemento: Agrupación de factores que hace parte de un componente.

Entorno: Ambiente, contexto. Lo que rodea; territorio o conjunto de lugares que rodean a otro.

Evaluación de Riesgos: proceso utilizado para determinar la magnitud de los riesgos en una organización, con relación a uno criterios determinados.

Evento: Suceso; particularmente suceso posible.

Frecuencia del riesgo: medida estadística del número de veces que se presenta un riesgo en un período de tiempo.

Indicadores de riesgo: conjunto de variables cuantitativa y/o cuantitativas que se constituyen en herramientas para realizar el monitoreo de los riesgos.

Identificación de riesgos: proceso para reconocer si existe un riesgo y definir sus características.

Impacto: Cambio logrado en la situación de la comunidad como resultado del producto de un proceso. Es el nivel más elevado o la finalidad última del proceso y donde se genera la totalidad de los beneficios previstos. Es equivalente a Valor Agregado. En el elemento Valoración de Riesgos, es la magnitud del deterioro en la situación de la entidad, como resultado de la materialización de un riesgo.

Mapa de Riesgos Institucional: Contiene a nivel estratégico los mayores riesgos a los cuales está expuesta la entidad, se alimenta con los riesgos residuales de cada uno de los procesos, los cuales pueden afectar el cumplimiento de la misión institucional y objetivos de la entidad. En este mapa se deberán incluir los riesgos identificados como posibles actos de corrupción, en cumplimiento del artículo 73 de la Ley 1474 de 2011.

Mapa de Riesgos por Proceso: Recoge los riesgos identificados para cada uno de los procesos, los cuales pueden afectar el logro de sus objetivos.

Medidas de tratamiento: opciones contempladas para manejar o administrar un riesgo. Respuestas ante los riesgos.

Monitoreo de riesgos: Evaluación permanente del comportamiento de los riesgos, a través de indicadores cualitativos o cuantitativos.

Peligro: Fuente, situación o acto con un potencial de daño en términos de lesión o enfermedad o una combinación de estas.
Pérdida: consecuencia negativa que puede ocasionar un riesgo, sea financiera o de otro tipo.

Plan: Proyecto, programa de las cosas que se van a hacer y de cómo hacerlas.

Políticas: Principios que sirven de guía y dirigen los esfuerzos de una organización para alcanzar sus objetivos.

Políticas de Administración de Riesgos: guía para la toma de decisiones o criterios de acción que rigen a todos los empleados con relación a la administración de riesgos. Trasmiten la posición de la dirección respecto de su actitud ante los riesgos y fijan lineamientos para la protección de los recursos, conceptos de calificación de riesgos, prioridades en la respuesta y la forma de administrarlos.

Posibilidad: condición o característica para que llegue a ocurrir un hecho.

Probabilidad: medida estadística (expresada en un porcentaje o una razón), de la posibilidad de ocurrencia de un riesgo.

Procedimiento: Método o sistema estructurado para ejecutar algunas cosas. Acto o serie de actos u operaciones con que se hace una cosa.

Proceso: Conjunto de actividades que realiza una organización, mediante la transformación de unos insumos, para crear, producir y entregar sus productos, de tal manera que satisfagan las necesidades de sus clientes.

Reducir: medida de tratamiento de los riesgos que busca disminuir la posibilidad de ocurrencia de un riesgo, sus consecuencias o ambas.

Responsable: Que es consciente de sus obligaciones y actúa conforme a ellas.

Riesgo: 1. Evento capaz de poner en peligro el cumplimiento de los objetivos de la Entidad Pública con eficiencia, eficacia y calidad. 2. La posibilidad de que ocurra dicho evento.

Riesgo aceptable: aquel que se considera normal para una actividad determinada. Es el riesgo que tiene una probabilidad o frecuencia de ocurrencia muy baja y su impacto leve.
Seguimiento

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 de gestión: Es aquel riesgo que se puede dar como consecuencia del quehacer diario de la entidad entre ellos tenemos riesgos de Operativos, riesgos de seguridad de la información, riesgos ambientales y riesgos de seguridad y salud en el trabajo

Riesgos de seguridad en las personas: El riesgo de seguridad personal son riesgos asociados a aquellas amenazas que podrían afectar al personal, los activos u operaciones de la Unidad por la acción directa e indirecta de grupos armados, delincuencia común etc.

Riesgo inherente: Es aquel al que se enfrenta una entidad en ausencia de acciones de la dirección (controles) para modificar su probabilidad o impacto; es decir, es la valoración del riesgo sin tener en cuenta los controles establecidos para este.

Riesgo inaceptable: riesgo que por la evaluación de su probabilidad y de sus consecuencias requiere ser evitado o eliminado, porque puede traer consecuencias catastróficas.

Riesgo residual: Nivel de riesgo que permanece luego determinar medidas de tratamiento del riesgo.

Seguimiento: Es la observación minuciosa de la evolución y desarrollo de un proceso.

Servidores públicos: Son los miembros de las corporaciones públicas, los empleados y trabajadores del Estado y de sus entidades descentralizadas territorialmente y por servicios.

Socializar: Compartir la información con todos los funcionarios del grupo al que pueda interesar.

Subsistema: Agrupación de Componentes que hace parte de un Sistema.

Valoración de riesgos: Es un Elemento del Componente Administración de Riesgos que comprende el conjunto de acciones por las cuales se estima la magnitud de los riesgos (frecuencia e impacto), y se evalúan para determinar si pueden aceptarse o no.

5. DESARROLLO

I. MARCO LEGAL

- Constitución Política de Colombia. Artículos 209 y 269.
- Ley 87 de 1993: "Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del Estado y se dictan otras disposiciones". (Modificada parcialmente por la Ley 1474 de 2011). Artículo 2 objetivos de control interno: literal a). Proteger los recursos de la organización, buscando su adecuada administración ante posibles riesgos que los afectan. Literal f). Definir y aplicar medidas para prevenir los riesgos, detectar y corregir las desviaciones que se presenten en la organización y que puedan afectar el logro de los objetivos.
- Ley 489 de 1998: "Estatuto básico de organización y funcionamiento de la Administración Pública. Capítulo VI. Sistema Nacional de Control Interno.
- Decreto 2145 de 1999: "Por el cual se dictan normas sobre el Sistema Nacional de Control Interno de las Entidades y Organismos de la Administración Pública del orden nacional y territorial y se

dictan otras disposiciones." (Modificado parcialmente por el Decreto 2593 del 2000 y por el Art. 8° de la Ley 1474 de 2011).

- Decreto 1537 de 2001: "Por la cual se reglamenta parcialmente la Ley 87 de 1992 en cuanto a elementos técnicos y administrativos que fortalecen el Sistema de control interno de entidades y organismos del estado". El párrafo del Artículo 4° señala los objetivos del sistema de control interno (…) define y aplica medidas para prevenir los riesgos, detectar y corregir las desviaciones (…) y en su Artículo 3° establece el rol que debe desempeñar las oficinas de control interno (…) que se enmarca en cinco tópicos (…) valoración de riesgos. Así mismo establece en su Artículo 4° la administración de riesgos, como parte integral del fortalecimiento de los sistemas de control interno en las entidades públicas (…)

- 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 prestadores de servicio".

- 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.

- Decreto 0943 de 2014: "Por medio del cual se actualiza el Modelo Estándar de Control Interno MECI" y se presenta el manual técnico del modelo estándar de control interno para el Estado colombiano MECI 2014. Numeral 1.3 Componente de administración del riesgo.

- Norma Técnica de Calidad en la Gestión Pública (NTCGP) 1000 de 2009 " Sistema de Gestión de la Calidad para la rama ejecutiva del poder público y otras entidades prestadoras de servicios". Numerales 4.1 Requisitos generales, 5.6.2 Revisión por la dirección, 7.5.1 Control de la producción y de la prestación del servicio y 8.5.3 Acción preventiva.

- Norma Técnica Colombiana de Gestión de Riesgos - NTC 31000 de febrero 16 de 2011.

- Resolución 0479 del 30 de julio de 2014 "por la cual se adopta el Modelo Estándar de Control Interno MECI 2014 en la Unidad para la Atención y Reparación Integral a las Víctimas y se deroga la Resolución 0899 del 03 de septiembre de 2013".

- La documentación que sobre el tema emita el Departamento Administrativo de la Función Pública (DAFP).

- La documentación que sobre el tema emita la Secretaria de Transparencia de la Presidencia de la Republica.

II. Generalidades de la Administración de Riesgos

1. Definición

La Administración de riesgos es necesaria debido a la incertidumbre y la posibilidad que tienen las Entidades de verse enfrentadas a circunstancias, internas y externas, que puedan afectar el logro de sus objetivos[1]

La administración de riesgos es un proceso desarrollado por la Alta Dirección de la Entidad y por todo el personal para proporcionar un aseguramiento razonable con respecto al logro de los objetivos. El enfoque de riesgos se determina con el uso de la metodología y con la evaluación de los riesgos como parte del proceso de planeación.

2. Objetivos

El objetivo primordial de la Administración de riesgos es crear una cultura de **PREVENCIÓN Y CONTROL** para que los eventos inesperados causen el mínimo impacto posible.

Entre los objetivos específicos se tienen:

- Prevenir o mitigar cualquier pérdida económica que pueda generar la ocurrencia de los riesgos, a través del diseño e implementación de mapas de riesgo, dirigidos a mantener y mejorar la efectividad de los controles existentes.
- Proteger a los funcionarios contra accidentes que pueden causar lesiones, daños serios o muerte, mejorando y haciendo más seguras las condiciones de trabajo e implementando medidas preventivas y de protección.
- Utilizar los recursos humanos, físicos y financieros en forma eficaz que contribuyan al cumplimiento de los objetivos propuestos.
- Mantener la buena imagen y las buenas relaciones de la entidad con sus grupos de interés.
- Determinar la estrategia de comunicación que permitirá afrontar las crisis y los eventos inesperados.

3. Beneficios

La Administración de riesgos contribuye a gestionar los riesgos para alcanzar los objetivos en todos los niveles institucionales.

[1] (Guía para la Administración del riesgo. Departamento Administrativo de la Función Pública, 2015)

Los beneficios de la Administración de riesgos son:

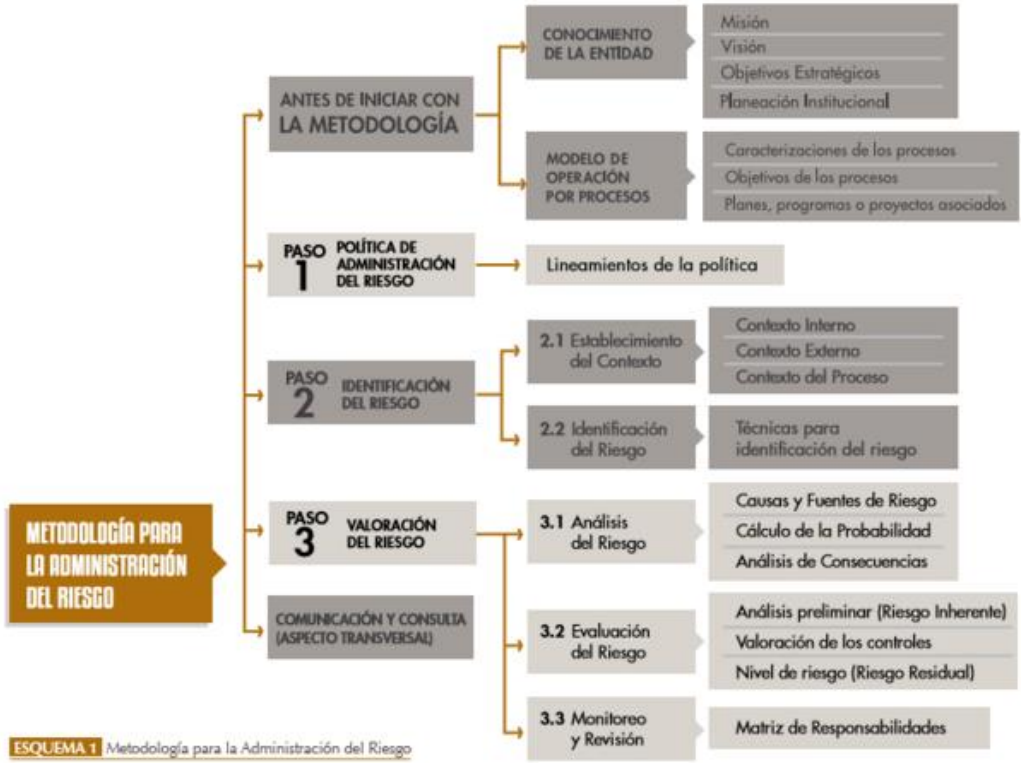
- Contribuir al cumplimiento de los objetivos de la Unidad y de cada proceso.
- Consolidar la información de los riesgos para su análisis y mitigación.
- Identificar los riesgos más relevantes en cada proceso y los estratégicos de la Unidad
- Saber cómo actuar en situaciones de crisis.
- Mejorar la cultura organizacional propiciando espacios para la participación y discusión sobre los aspectos a mejorar.
- Fortalecer el Sistema Integrado de Gestión de la Unidad.
- Contribuir a una planificación estratégica más efectiva que tiene en cuenta los riesgos estratégicos.

III. Metodología Administración del Riesgo

La metodología se diseñó teniendo en cuenta los lineamientos del Modelo Estándar de Control Interno - MECI 2014, la Guía para Administración de Riesgos del DAFP. Guía para la gestión del riesgo de corrupción de la Secretaria de Transparencia de la Presidencia de la Republica y la NTC 31000 de Gestión de Riesgos de ICONTEC , GTC 45, NTC 14001: 2015, NTC 27001: 2013 y *contempla seis capítulos que en su orden son:*

I. Conocimiento previo
II. Política de Administración de Riesgos
III. Etapas de la Administración del Riesgo
IV. Monitoreo y revisión
V. Seguimiento
VI. Divulgación, comunicación y consulta
VII. Roles y responsabilidades.

A. Metodología de administración de riesgos[2]



ESQUEMA 1 Metodología para la Administración del Riesgo

Como resultado de la aplicación de la metodología se obtiene el Mapa de Riesgos Institucional y el mapa de riesgos por procesos.

Los mapas de riesgos se elaboran con la participación activa de los directivos y servidores públicos de todos los procesos de la Unidad y el acompañamiento del y con el apoyo de los enlaces INTEGRA del Sistema Integrado de Gestión de la Unidad.

Para la identificación de los riesgos, se tomará como base toda la documentación disponible de la Entidad, a fin de registrar todos los riesgos existentes y que puedan afectar el normal funcionamiento de los procesos (ejemplo: análisis de contexto, informes de Auditorias, informes de seguimiento a los mapas de riesgos, los riesgos materializados, etc.).

De acuerdo al marco metodológico usado para la construcción de este documento se encontró que la Metodología de Administración de Riesgos de Departamento Administrativo de la Función

[2] (Guía para la Administración del riesgo. Departamento Administrativo de la Función Pública, 2015)

Pública y Guía para la gestión del riesgo de corrupción de la Secretaria de Transparencia de la Presidencia de la Republica aplican de manera similar la metodología de administración de riesgos para los riesgos de gestión y los de corrupción, la única diferencia encontrada fue en la etapa de valoración del riesgo, por esa razón fue necesario desarrollar al interior de esta metodología un capitulo independiente para la etapa de valoración para los riesgos de corrupción. Sin embargo los demás aspectos y etapas serán tratados de manera integral para los dos tipos de riesgos.

1. Conocimiento previo

Para implementar a metodología de administración de riesgos es necesario tener conocimiento sobre:

a. **La planeación estratégica de la Unidad**: (misión, visión, objetivos estratégicos)
b. **Modelo de operación por procesos:** (cadena de valor, mapa de procesos, caracterización y objetivos de los procesos y procedimientos)
c. **Sistema Integrado de Gestión y sus componentes**.
d. **Política de Administración de Riesgos.** Alcance, nivel de aceptación etc.
e. **Contexto estratégico de la Unidad.** Contexto interno y externo
f. **Partes interesadas.** Dentro del contexto estratégico se establecen las relaciones que la Unidad tiene con las partes interesadas ya sean internas o externas, entendidas como entes o personas que están o perciben que pueden ser afectados por una decisión o una actividad de la Unidad. Según la planeación estratégica de la Unidad, las partes interesadas están clasificadas en 5 grupos, así:

- **Víctimas del conflicto armado:** Personas que individual o colectivamente hayan sufrido un daño de manera directa por hechos que guarden relación con el conflicto armado.
  Por hecho victimizante, encontramos principalmente:
  - Hogares desplazados
  - Personas víctimas de homicidios
  - Denunciantes de abandono de tierras
  - Víctimas de secuestro
  - Víctimas de desaparición forzada
  - Víctimas de violencia sexual en el marco del conflicto armado
  - Víctimas de minas antipersonal
  - NNA víctimas de reclutamiento forzoso
  - Sujetos colectivos (grupos, comunidades y organizaciones, sujetos étnicos)
  - Miembros de la fuerza pública víctimas del conflicto armado

- **Entidades públicas y privadas del orden nacional:** Conjunto de entidades públicas del nivel gubernamental y estatal en el orden nacional y territorial y demás organizaciones públicas o privadas, encargadas de formular o ejecutar los planes, programas, proyectos y acciones específicas, que tiendan a la atención y reparación integral de las víctimas.

- **Entidades territoriales:** Conjunto de entidades públicas del nivel gubernamental y estatal en el orden territorial y demás organizaciones públicas o privadas, encargadas de formular o

ejecutar los planes, programas, proyectos y acciones específicas, que tiendan a la atención y reparación integral de las víctimas. Es importante la articulación Nación-Territorio.

- **Sociedad y Comunidad Internacional:** conformado por diversos grupos que son:
    - Ciudadanos colombianos y colombianas
    - Sociedad civil organizada
    - Grupos diferenciales
        - Niños, niñas y adolescentes
        - Personas mayores
        - Población LGBTI
        - Mujeres y Hombres
        - Afrodescendientes, Indígenas y Campesinos
        - Personas con discapacidad y/o habilidades diversas
    - Cooperantes institucionales de acuerdo a clasificación APC
    - Sistema Internacional de Protección de DDHH
    - Cooperantes no institucionalizados o individuales
    - Países receptores (consulados o defensorías)

- **Unidad (cliente interno):** está conformada por los servidores públicos de la Unidad para la Atención y Reparación Integral a las Víctimas y sus familias, así como el personal vinculado a través de contratación de operadores específicos.

2. Política de administración del riesgo

"*La Unidad administra, gestionando integralmente sus riesgos en los procesos estratégicos, misionales, de apoyo y de control, a fin de optimizar su eficacia y eficiencia a través de la identificación, análisis y valoración de riesgos y la definición de estrategias para su mitigación, majeño de crisis y comunicaciones estratégicas*".

Esta política que en su conjunto contribuye al proceso de toma de decisiones de manera oportuna y con ello evitar la materialización del riesgo que en un momento dado puede afectar o impedir el normal desarrollo de los procesos y/o el cumplimiento de los objetivos estratégicos de la Entidad, además ayuda a fortalecer la cultura de confianza, colaboración e innovación para garantizar una atención digan respetuosa y diferencial a las víctimas.

A. Alcance

La política de administración de riesgos aplica a todos los procesos a de nivel Nacional y a las Direcciones Territoriales de la Unidad para la Atención y Reparación a las Víctimas.

B. Nivel de Aceptación del Riesgo

De acuerdo a la Metodología de Administración de riesgo en la etapa de valoración del riesgo debe analizarse y evaluarse la probabilidad y el impacto del riesgo. De acuerdo a esto los riesgos pueden ubicarse en Zona de riesgo Extrema, Alta, Moderada y Baja, estos niveles se explican con mayor detalle en el numeral 3.3 y 3.4. del presente documento.

De acuerdo a la guía para la gestión del riesgo de corrupción[3], es necesario que las Entidades establezcan un nivel de tolerancia y aceptación de los riesgos. La Unidad para la Atención y Reparación Integral a las Víctimas ha establecido como nivel de aceptación de riesgos, todos los riesgos que se ubiquen en un nivel bajo, ya que los controles son suficientes y nivel de riesgo sería aceptable.

Periodicidad para el seguimiento del mapa de riesgos

La Unidad para las Víctimas determina que el seguimiento del mapa de riesgos de proceso e institucional lo realizará la oficina de Control Interno y tendrá una periodicidad cuatrimestral con corte a 30 de abril, 31 de agosto y 31 de diciembre de la vigencia correspondiente. La etapa de monitoreo del mapa de riesgos es responsabilidad de los procesos y del Equipo Nacional de Gestión y Seguimiento de Riesgos, crisis y comunicaciones estratégicas el cual tendrá periodicidad cuatrimestral con corte a corte al 31 de marzo, al 31 de Julio y 30 de Noviembre. Con respecto al monitoreo de la materialización de los riesgos es responsabilidad de líder del proceso y debe generar un reporte permanente de los riesgos materializados. Estas etapas de la metodología serán tratadas a mayor detalle en el capítulo 3 de este documento.

C. Niveles de responsabilidad

Los niveles de responsabilidad sobre las actividades de cada una de las etapas de la metodología se encuentran establecidas en la matriz de Roles y Responsabilidades ubicada en el capítulo 8 de este documento.

D. Actualización metodológica

La Metodología de Administración de Riesgos de la Unidad está sujeta a las orientaciones que sobre la materia determine el Departamento Administrativo de la Función Pública, la Secretaria de transparencia de la Presidencia de la Republica y las normas o estándares nacionales que se establezcan sobre el particular.

E. Documentación

La documentación sobre Administración de Riesgos en la Unidad, que incluye la presente metodología, el manual de manejo de crisis y comunicaciones estratégicas, el procedimiento correspondiente y los instrumentos técnicos que la soportan, estarán disponibles en la intranet de la Unidad, en el proceso de Direccionamiento Estratégico, para consulta permanente de todos los servidores públicos de la Entidad.

F. Mecanismos de comunicación

El proceso de Direccionamiento Estratégico impulsará la sensibilización, socialización e interiorización de la administración de riesgos, a través de los diferentes mecanismos de

[3] (Guía para la gestión del riesgo de corrupción. Presidencia de la República, 2015)

comunicación interna con que cuenta la Unidad, para promover la cultura del autocontrol y de la prevención del riesgo.

G. Mapas de riesgos por procesos y mapa de riesgos institucional

Los mapas de riesgos se elaboran con la participación activa de los directivos y servidores públicos de todos los procesos de la Unidad y el acompañamiento de la Oficina Asesora de Planeación, particularmente con el apoyo de los enlaces INTEGRA del Sistema Integrado de Gestión de la Unidad, quienes además facilitarán y apoyarán su monitoreo.

Para la identificación de los riesgos, se tomará como base toda la documentación disponible de la Entidad, a fin de registrar todos los riesgos existentes y que puedan afectar el normal funcionamiento de los procesos (ejemplo: análisis de contexto, informes de Auditorias, informes de seguimiento a los mapas de riesgos, los riesgos materializados, etc.).

Contiene los riesgos a los cuales está expuesta la entidad, permitiendo conocer el plan de respuesta ante ellos, es decir, aquellos riesgos residuales moderados, altos o extremos de cada proceso, que pueden afectar el cumplimiento de la misión o los objetivos de la Unidad.

Para las Direcciones territoriales se construirá un mapa de riesgos propio, el cual se trabajará después de construidos los mapas de riesgos de los procesos, pero bajo la misma metodología y condiciones de los mapas de riesgos de procesos.

3. Etapas de la administración del riesgo

3.1 Establecimiento del contexto

La definición del contexto estratégico, se refiere a la identificación de los aspectos o factores internos, externos y de proceso, que pueden afectar positiva o negativamente a la entidad. A partir de estos aspectos se establecen las causas de los riesgos a identificar y que pueden afectar el cumplimiento de sus objetivos. Esto se da a partir de la observación, distinción y análisis de las circunstancias internas y externas.

a. Contexto externo

Hace referencia a los factores o condiciones del entorno externo, que pueden afectar el cumplimiento del objetivo de la Unidad.

Se pueden considerar factores como:

- Económicos: Disponibilidad de capital, liquidez, mercados financieros, desempleo, competencia, Recursos públicos no regulados efectivamente Políticos y legales: Cambios de gobierno, legislación, normatividad compleja, políticas públicas, regulación.
- Sociales: Demografía, responsabilidad social, orden público, actores corruptos.

- Tecnológicos: Avances en tecnología, acceso a sistemas de información externos, gobierno en línea.
- Medioambientales: Emisiones y residuos, energía, catástrofes naturales, desarrollo sostenible
- Comunicación externa: Mecanismos utilizados para entrar en contacto con los usuarios o ciudadanos, canales establecidos para que el mismo se comunique con la entidad.

b. Contexto interno

Hace referencia a los factores o condiciones del entorno interno, que pueden afectar el cumplimiento del objetivo de la Unidad. Se pueden considerar factores como:

- Financieros: Presupuesto de funcionamiento, recursos de inversión, infraestructura, capacidad instalada, Costos administrativos
- Talento humano: Competencia del personal, disponibilidad del personal, Identificación de peligros seguridad y salud en el trabajo, Discrecionalidad del personal en ejercicio de sus funciones.
- Procesos: Capacidad, diseño, ejecución, proveedores, entradas, salidas, gestión del conocimiento, Fallas en los diseños de los procesos y procedimientos de los trámites
- Tecnología: Integridad de datos, disponibilidad de datos y sistemas, desarrollo, producción, mantenimiento de sistemas de información, Deficiencias tecnológicas en la gestión de tramites e identificación de vulnerabilidades y amenazas que puedan afectar los activos de información.
- Estratégicos: Direccionamiento estratégico, planeación institucional, liderazgo, trabajo en equipo, cultura organizacional.
- Comunicación interna: Canales utilizados y su efectividad, flujo de la información necesaria para el desarrollo de las operaciones.

En esta etapa se deben establecer las fuentes o factores de riesgo, los eventos, sus causas y sus consecuencias. Para el análisis se pueden involucrar datos históricos, análisis teóricos, opiniones informadas y expertas y las necesidades de las partes involucradas[4]. Como herramienta básica para el análisis del contexto del proceso se sugiere utilizar las caracterizaciones de los mismos, donde es posible contar con este panorama.

Para el análisis del contexto Interno y externo de la Unidad se realizarán sesiones de trabajo lideradas por Direccionamiento Estratégico y los representantes de los procesos junto a los cuales se determinaran las fortalezas y debilidades, las oportunidades y amenazas frente a los aspectos económicos, políticos tecnológicos, comunicación interna y externa, medio ambientales, legales, financieros, estratégicos y cultura organizacional. Para controlar y valorar estos factores utilizaremos la herramienta POAM (Perfil de Oportunidades y Amenazas del Medio), la cual se formalizara por medio de un formato cuyo resultado servirá de insumo en la construcción de mapa de riesgos de la Unidad.

[4] (Norma Técnica Colombiana NTC ISO 31000, Instituto Colombiano de Normas Técnicas ICONTEC, 2011)

3.2 Identificación del Riesgo

La identificación de los riesgos se realiza determinando las causas, consecuencias y tipo de riesgo con base en el análisis del contexto interno, externo y del proceso, las fuentes de riesgo y los eventos que pueden afectar el logro de los objetivos. Preguntas clave para la identificación del riesgo

¿Qué puede suceder? – Descripción del riesgo
¿Por qué puede suceder? - Causas
¿Qué pasaría si sucede?- Consecuencias

Importante

- Para la identificación de los riesgos de corrupción, se deben identificar los procedimientos o tareas que cuenten con los siguientes factores críticos, ya que su presencia puede aumentar la posibilidad de que ocurra un hecho de corrupción:

  - Oportunidad: Se refiere a las fallas de diseño del procedimiento donde se abren espacios de discrecionalidad de los servidores que pueden generar espacios de corrupción. Está asociado a la falta de controles internos y externos que sean efectivos.

  - Presión: Se refiere al hecho de ejercer influencia/obligar a una persona a tomar una decisión o a realizar una acción. Con respecto a lo hechos de corrupción puede darse por actores criminales o situaciones de presión económica y social para la ejecución de trámites o procedimientos al interior de la entidad. Esto se presenta generalmente por una actitud del individuo que justifica actos por fuera de la integridad pública bajo una valoración de ética por fuera de la finalidad de los principios del servicio público.
  - Responsabilidad: Se refiere a las fallas en la ética, integridad, cumplimiento y compromiso con lo público, afectando el cumplimiento del objetivo de la entidad.

- Para los riesgos de Seguridad y salud en el trabajo se usará como insumo para la identificación la Matriz de Identificación de Peligros, Valoración del Riesgo y Determinación de Controles la cual se explica a mayor detalle en el anexo 2 del presente documento.

- Para los riesgos de Seguridad de la información se como insumo para la identificación de los riesgos a nivel institucional de acuerdo al anexo 3 del presente documento.

a. Descripción del riesgo

En necesario hacer una corta descripción del riesgo dentro de la identificación. Es importante centrarse en los riesgos más significativos para la entidad relacionados con los objetivos de los procesos y los objetivos estratégicos.

Para la redacción del riesgo se deben tener en cuenta:

- Usar un lenguaje claro y común
- El riesgo no puede ser una negación
- La ausencia de control no es un riesgo
- La redacción del evento puede comenzar con la palabras falta, incumplimiento, omisión, retraso, colapso, perdida, inoportunidad, dificultad, imposibilidad, indisponibilidad, desviación y utilizando adjetivos calificativos asociados a alguna actividad del proceso tales como inadecuado, inoportuno, deficiente etc.

b. Determinación de las causa

Las causas son factores internos o externos; Son los motivos, medios o circunstancias que darían origen a la ocurrencia de los riesgos, cuyos agentes generadores pueden ser: personas, materiales, Instalaciones y entorno. Es posible establecer más de una causa como factor del riesgo a identificar.

Una clave para definir las causas es el uso de las palabras: falta de, ausencia de, fallas de, exceso de, etc. Palabras que conducen a deficiencias que pueden propiciar o permitir la ocurrencia de los riesgos. Como lo pueden ser falta de políticas de selección de proveedores, falta de normas para el proceso de compras, fallas en la selección del personal, carencia de procedimientos de validación y verificación del producto final, etc.

c. Determinación de las consecuencias

Las consecuencias son los efectos de la ocurrencia del riesgo sobre los objetivos de la entidad; generalmente, se dan sobre las personas o los bienes materiales o inmateriales con incidencias importantes tales como: daños físicos, sanciones, pérdidas económicas, de información, de bienes, de imagen, de credibilidad y de confianza, interrupción del servicio y daño ambiental.

Para el caso de la Unidad, se contemplan algunas categorías como guía para determinar las consecuencias: salud de personas, seguridad en las personas, credibilidad o imagen, operacional, seguridad en la información, legal y otros.

- **Afectación en la integridad de las personas.** En caso de materializarse, podría afectar la salud o la vida de los servidores públicos y/o contratistas que laboran en la Entidad.

- **Afectación en la credibilidad o imagen.** En caso de materializarse, podría afectar la credibilidad y buen nombre de la Entidad frente a las partes interesadas o dentro de la Entidad.

- **Operativa.** En caso de materializarse, podría afectar el desarrollo normal de los procesos, generando retrasos o incumplimiento en sus actividades, entre otros, fallas en los sistemas de información, desconocimiento de un procedimiento, problemas con la comunidad, etc.

- **Legal.** En caso de materializarse, la Unidad podría enfrentar consecuencias de tipo legal debido al incumplimiento de su función administrativa, ejecución presupuestal y normatividad aplicable.

- **Disciplinaria**: En caso de materializarse, podría generar procesos y sanciones disciplinarias

d. Tipos de riesgos

En la identificación del riesgo es necesario establecer el tipo de riesgo al cual nos enfrentamos, la Unidad sugiere algunos tipos de riesgos, los cuales se describen a continuación:

- **Riesgo de gestión/Operativos**: Comprenden riesgos provenientes del funcionamiento y operatividad de los sistemas de información institucional, de la definición de los procesos, de la estructura de la entidad, de la articulación entre dependencias.

- **Riesgo financiero:** Se relacionan con el manejo de los recursos de la entidad que incluye, la ejecución presupuestal, la elaboración de los estados financieros, los pagos, manejos de excedentes de tesorería y el manejo sobre los bienes de cada entidad.

- **Riesgos de seguridad de la información**: Son potenciales amenazas que pueden detonar una vulnerabilidad de un activo de información afectando su Integridad, confidencialidad y disponibilidad.

- **Riesgos de seguridad y salud en el trabajo**: Es la probabilidad de que un objeto material, sustancia o fenómeno pueda potencialmente desencadenar perturbaciones en la salud o integridad física del personal, así como en materiales y equipos.

- **Riesgos ambientales**: Es el riesgo que se puede presentar en forma de "perturbación" causada por la actividad (o inactividad) humana que lleva a la degradación o a la pérdida de la sostenibilidad.

- **Riesgos Financieros:** Se relacionan con el manejo de los recursos de la entidad que incluyen la ejecución presupuestal, la elaboración de los estados financieros, los pagos, manejos de excedentes de tesorería y el manejo sobre los bienes

- **Riesgo de público**. El riesgo de seguridad personal son riesgos asociados a aquellas amenazas que podrían afectar al personal, los activos u operaciones de la Unidad por la acción directa e indirecta de grupos armados, delincuencia común etc. Estos riesgos son una categoría especial de los riesgos de gestión que por su naturaleza estratégica serán trabajados e identificados desde la Alta dirección. Para efectos de la metodología estos riesgos solo se diferencian en la etapa de análisis de riesgo razón por la cual este tema se desarrollará en el anexo 2 del presente documento.

- **Riesgo de corrupción**. Relacionados con acciones, omisiones, uso indebido del poder, de los recursos o de la información para la obtención de un beneficio particular o de un tercero.

3.3. Valoración de los riesgos (Riesgos de Operativos, financieros, Seguridad de la información, Seguridad y salud en el trabajo, ambientales, financieros, públicos)

La valoración del riesgo consiste en establecer la probabilidad de ocurrencia del riesgo y el nivel de consecuencias o impacto, con el fin de estimar la zona de riesgo inicial (Riesgo Inherente). Incluye el análisis del riesgo y la valoración.

3.3.1. Análisis del Riesgo

El análisis de riesgo busca establecer la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto. Con el fin de estimar la zona de riesgo inicial, denominada riesgo inherente. Primero, se determina la probabilidad entendida como la posibilidad de ocurrencia del riesgo; segundo se determinan las consecuencias o nivel de impacto que puede ocasionar la materialización del riesgo y finalmente se estima el nivel de riesgo inherente.

Para efectos de la metodología el análisis de riesgos de seguridad personal la etapa de valoración se desarrollará de acuerdo al anexo 1 de este documento.

a. Calificación de la probabilidad

La probabilidad es la posibilidad de ocurrencia de un evento de riesgo y se mide según su frecuencia, es decir el número de veces en que pudo haberse presentado el evento en un periodo determinado.

La probabilidad para los riesgos de gestión, riesgos de seguridad de la información y riesgos ambientales se califica de acuerdo a los siguientes parámetros:

Tabla calificación de la probabilidad

Nivel	Descriptor	Descripción	Frecuencia
5	Casi seguro	Se espera que el evento ocurra en la mayoría de las Circunstancias	Más de 5 veces al año.
4	Probable	Es viable que el evento ocurra en la mayoría de las circunstancias	Al menos 3 veces en el último año.

3	Posible	El evento podrá ocurrir en algún momento	Al menos 1 vez en el último año.
2	Improbable	El evento puede ocurrir en algún momento	Al menos 1 vez en los últimos 2 años.
1	Rara vez	El evento puede ocurrir solo en circunstancias excepcionales (Poco comunes o anormales).	No se ha presentado en los últimos 2 años.

Fuente: Oficina de Planeación

b. Calificación del impacto

El impacto es la consecuencia o efecto que puede generar la materialización del riesgo. Para los riesgos de operativos, riegos de seguridad de la información y riesgos ambientales el Impacto se califica de acuerdo a los siguientes parámetros:

Tabla calificación del Impacto[5]

Niveles para calificar el Impacto	Escala	Impacto (consecuencias) Cuantitativo	Impacto (consecuencias) Cualitativo
CATASTRÓFICO	5	-Impacto que afecta la ejecución presupuestal en un valor mayor o igual al 50% -Pérdida de cobertura en la prestación de los servicios a las victimas mayor o igual al 20% -Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor mayor o igual al 20% -Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor mayor o igual al 20% del Presupuesto general de la entidad.	- Interrupción de las operaciones de la Entidad por más de Cinco (5) días. - Intervención por parte de un ente de control u otro ente regulador. - Pérdida de Información crítica para la entidad que no se puede recuperar. - Incumplimiento en las metas y objetivos institucionales afectando de forma grave la ejecución presupuestal. - Imagen institucional afectada en el orden nacional o territorial por actos o hechos de corrupción comprobados.

[5] (Guía para la Administración del riesgo. Departamento Administrativo de la Función Pública, 2015)

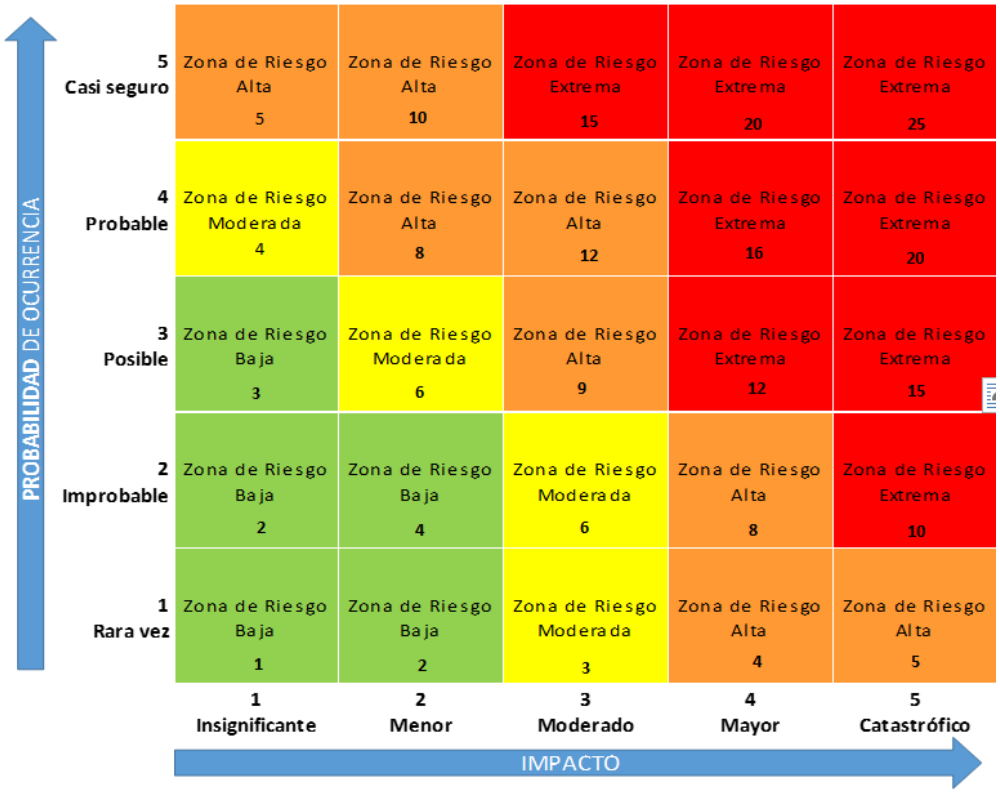
MAYOR	4	-Impacto que afecte la ejecución presupuestal en un valor mayor o igual al 10% -Pérdida de cobertura en la prestación de los servicios a las víctimas mayor o igual al 10% -Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor mayor o igual al 10% -Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor mayor o igual al 20% del presupuesto general de la entidad.	- Interrupción de las operaciones de la Entidad por más de dos (2) días. - Pérdida de información crítica que puede ser recuperada de forma parcial o incompleta. - Sanción por parte del ente de control u otro ente regulador. - Incumplimiento en las metas y objetivos institucionales afectando el cumplimiento en las metas de gobierno. - Imagen institucional afectada en el orden nacional o territorial por incumplimientos en la prestación del servicio a los usuarios o ciudadanos.
MODERADO	3	-Impacto que afecte la ejecución presupuestal en un valor mayor o igual al 5%. -Pérdida de cobertura en la prestación de los servicios a las víctimas mayores o igual al 5%. -Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor mayor o igual al 5%. -Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor mayor o igual al 5% del presupuesto general de la entidad.	- Interrupción de las operaciones de la Entidad por un (1) día. - Reclamaciones o quejas de los usuarios que podrían implicar una denuncia ante los entes reguladores o una demanda de largo alcance para la entidad. - Inoportunidad en la información ocasionando retrasos en la atención a los usuarios. - Reproceso de actividades y aumento de carga operativa. - Imagen institucional afectada en el orden nacional o territorial por retrasos en la prestación del servicio a los usuarios o ciudadanos. - Investigaciones penales, fiscales o disciplinarias.

Menor	2	- Impacto que afecte la ejecución presupuestal en un valor menor al 5% - Pérdida de cobertura en la prestación de los servicios a las víctimas menor al 10% - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor menor al 5% - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor menor al 5% del presupuesto general de la entidad.	- Interrupción de las operaciones de la Entidad por algunas horas. - Reclamaciones o quejas de los usuarios que implican investigaciones internas disciplinarias. - Imagen institucional afectada localmente por retrasos en la prestación del servicio a los usuarios o ciudadanos.
Insignificante	1	- Impacto que afecte la ejecución presupuestal en un valor menor o igual al 1% - Pérdida de cobertura en la prestación de los servicios a las víctimas menor o igual al 1% - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor menor o igual al 1% - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor menor o igual al 1%	- No hay interrupción de las operaciones de la entidad. - No se generan sanciones económicas o administrativas. - No se afecta la imagen institucional de forma significativa.

c. Determinación del riesgo inherente

Para estimar el nivel de riesgo inicial, los valores determinados para la probabilidad y el impacto o consecuencias se cruzan en la siguiente matriz de riesgo, con el fin de determinar la zona de riesgo en la cual se ubica el riesgo identificado. Este primer análisis del riesgo se denomina Riesgo Inherente y se define como aquél al que se enfrenta una entidad en ausencia de acciones por parte de la Dirección para modificar su probabilidad o impacto.

Tabla calificación riesgos de gestión[6]



3.3.2. Evaluación del riesgo

En esta fase se busca confrontar los resultados del análisis de riesgo inicial frente a los controles establecidos, con el fin de determinar la zona de riesgo final o riesgo residual.

Los controles son todas las medidas diseñadas para detectar y/o reducir un riesgo. En esta definición se utilizan tres conceptos claves el control como medida, la necesidad de detectar el riesgo y la necesidad de reducirlo. La definición de control como medida el entrenamiento en un puesto de trabajo, pasando por la definición de procedimientos, el desarrollo de planes de emergencia, la supervisión de una tarea, etc.

[6] (Guía para la Administración del riesgo. Departamento Administrativo de la Función Pública, 2015)

a. Evaluación de controles

En la evaluación de los controles se deben Identificar controles existentes, el responsable, el objetivo del control, como se lleva a cabo el control, cual es la evidencia de la ejecución del control, cuales el tipo de control, de acuerdo a esta información se debe determinar:

1) Descripción del control: En la descripción del control es necesario incluir:

- **Quien lleva a cabo el control**: Responsable
- **Cada cuanto se lleva a cabo el control:** Periodicidad/frecuencia
- **Que busca hacer el control**: Objetivo
- **Como se lleva a cabo**: Procedimiento al que pertenece
- **Cuál es la evidencia de la ejecución del control**: Soporte

1) Determinar su naturaleza: Si el control es preventivo o correctivo

Control Preventivo. Se establece para evitar que el evento suceda o minimizar el efecto de su materialización, su diseño y aplicación debe hacerse con asocio a otro tipo de controles, porque no son suficientes por sí mismos. Requieren de un mantenimiento periódico para conservar su eficacia. Algunos controles preventivos pueden ser:

- Acceso restringido.
- Procedimientos formales aplicados.
- Aseguramiento de la calidad, gestión y normalización.
- Claves de acceso.
- Condiciones contractuales.
- Distribución de funciones.
- Estandarización - SGC - Sistema documental.
- Firmas autorizadas.
- Gestión de proyectos.
- Inspección y procesos de control.
- Instructivos y guías.
- Investigación y desarrollo, desarrollo tecnológico.
- Mantenimiento preventivo.
- Medicina preventiva.
- Políticas de seguridad.
- Programa de selección de personal.
- Programas de capacitación y entrenamiento.
- Revisión formal de requisitos, especificaciones, diseño, ingeniería y operaciones.
- Rotación de funciones.
- Supervisión.
- Técnicas de control.
- Vigilancia.

Control correctivo. Está dirigido a corregir las desviaciones y prevenir de nuevo su ocurrencia. La guía de administración de riesgos define el control correctivo como aquellos que permiten el restablecimiento de la actividad después de ser detectado un evento no deseable; también permite la modificación de las acciones que propiciaron su ocurrencia. Algunos controles correctivos pueden ser:

- Actualización de procedimientos – sistema documental. (Se considera control correctivo cuando al materializarse el riesgo obliga a revisar y ajustar los procedimientos que le apliquen).
- Planes de recuperación de desastres.
- Procedimientos para correcciones de errores.

2) **Determinar si los controles están documentados:** Establecer si el control se encuentra o no documentado, conocer cómo se lleva a cabo el control, quién es el responsable de su ejecución y cuál es la periodicidad para su ejecución, lo cual determinará las evidencias que van a respaldar la ejecución del mismo

3) **Establecer si el control que se implementa:** Es automático o manual.

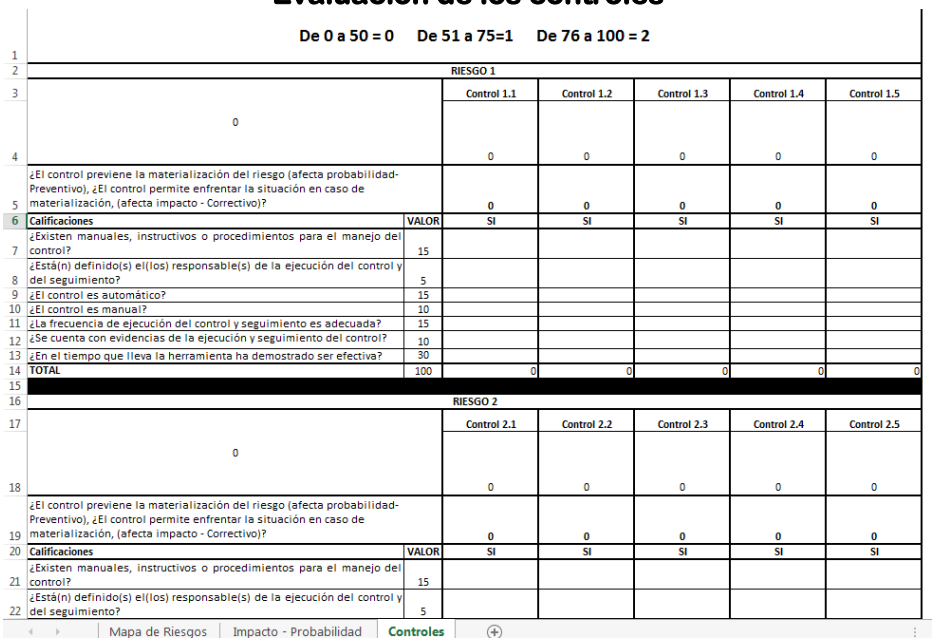
   - **Controles automáticos**: Son aquellos que utilizan herramientas tecnológicas como sistemas de información o software que permiten incluir contraseñas de acceso, o con controles de seguimiento a aprobaciones o ejecuciones que se realizan a través de éste, generación de reportes o indicadores entre otros. Este tipo de controles suelen ser más efectivos en algunos ámbitos, dados su complejidad.

   - **Controles manuales:** Políticas de operación aplicables, autorizaciones a través de firmas o confirmaciones vía correo electrónico, archivos físicos, consecutivos, listas de chequeo, controles de seguridad con personal especializado, entre otros.

4) **Determinar si los controles se están aplicando en la actualidad:** Si se encuentran aplicados y si han sido efectivos para minimizar el riesgo.

Para realizar el análisis y evaluación de los controles, se ha determinado el siguiente cuestionario, el cual está incluido en el formato para el levantamiento del mapa de riesgos I de la unidad en la hoja "Controles".

Evaluación de los controles



1			De 0 a 50 = 0	De 51 a 75=1	De 76 a 100 = 2		
2	RIESGO 1						
3			Control 1.1	Control 1.2	Control 1.3	Control 1.4	Control 1.5
4	0		0	0	0	0	0
5	¿El control previene la materialización del riesgo (afecta probabilidad- Preventivo), ¿El control permite enfrentar la situación en caso de materialización, (afecta impacto - Correctivo)?		0	0	0	0	0
6	Calificaciones	VALOR	SI	SI	SI	SI	SI
7	¿Existen manuales, instructivos o procedimientos para el manejo del control?	15					
8	¿Está(n) definido(s) el(los) responsable(s) de la ejecución del control y del seguimiento?	5					
9	¿El control es automático?	15					
10	¿El control es manual?	10					
11	¿La frecuencia de ejecución del control y seguimiento es adecuada?	15					
12	¿Se cuenta con evidencias de la ejecución y seguimiento del control?	10					
13	¿En el tiempo que lleva la herramienta ha demostrado ser efectiva?	30					
14	TOTAL	100	0	0	0	0	0
15							
16	RIESGO 2						
17			Control 2.1	Control 2.2	Control 2.3	Control 2.4	Control 2.5
18	0		0	0	0	0	0
19	¿El control previene la materialización del riesgo (afecta probabilidad- Preventivo), ¿El control permite enfrentar la situación en caso de materialización, (afecta impacto - Correctivo)?		0	0	0	0	0
20	Calificaciones	VALOR	SI	SI	SI	SI	SI
21	¿Existen manuales, instructivos o procedimientos para el manejo del control?	15					
22	¿Está(n) definido(s) el(los) responsable(s) de la ejecución del control y del seguimiento?	5					

Mapa de Riesgos | Impacto - Probabilidad | Controles

Fuente Oficina de Planeación

b. Determinación del Riesgo Residual

Se comparan los resultados obtenidos del riesgo inherente con los controles establecidos, para Establecer la zona del riesgo final o riesgo residual. Se califica de acuerdo con la siguiente tabla. De acuerdo al resultado obtenido los rangos de calificación de los controles son:

Rangos de calificación de los controles	Cuadrantes a disminuir
Entre 0-50	0
Entre 51-75	1
Entre 76-100	2

Esta calificación nos permite establecer la disminución del nivel de la probabilidad o del impacto del riesgo dependiendo del tipo de control:

- Si el control es preventivo se disminuye únicamente la probabilidad en el número de cuadrantes de acuerdo con la calificación obtenida por el control.
- Si el control es correctivo se disminuye únicamente el Impacto en el número de cuadrantes de acuerdo con la calificación obtenida por el control.

Si el control no genera ningún efecto en la probabilidad o impacto, debe ser eliminado o en su defecto debe generarse una acción en el plan de respuesta que permita en el futuro mejorar su calificación.

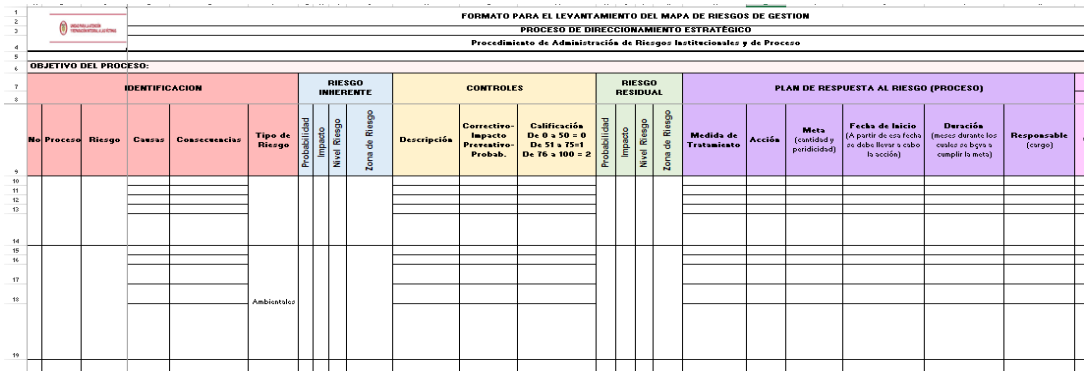
Nota:

*Si existen más de dos controles del mismo tipo el valor de la disminución será un promedio de la calificación de los controles.

3.3.3 Construcción del mapa de riesgos de Gestión

La información sobre los resultados de las etapas de Identificación y valoración, así como la información sobre el plan de respuesta, se registran el formato para el levantamiento de mapa de riesgos del proceso de la siguiente manera:

Mapa de riesgos de gestión


FORMATO PARA EL LEVANTAMIENTO DEL MAPA DE RIESGOS DE GESTION

PROCESO DE DIRECCIONAMIENTO ESTRATÉGICO

Procedimiento de Administración de Riesgos Institucionales y de Proceso

OBJETIVO DEL PROCESO:

IDENTIFICACION						RIESGO INHERENTE				CONTROLES				RIESGO RESIDUAL				PLAN DE RESPUESTA AL RIESGO (PROCESO)					
No	Proceso	Riesgo	Causas	Consecuencias	Tipo de Riesgo	Probabilidad	Impacto	Nivel Riesgo	Zona de Riesgo	Descripción	Correctivo-Impacto Preventivo-Probab.	Calificación De 0 a 50 = 0 De 51 a 75=1 De 76 a 100 = 2		Probabilidad	Impacto	Nivel Riesgo	Zona de Riesgo	Medida de Tratamiento	Acción	Meta (cantidad y periodicidad)	Fecha de inicio (A partir de esa fecha se debe llevar a cabo la acción)	Duración (meses durante los cuales se hará la meta)	Responsable (cargo)
					Ambientales																		

Fuente Oficina de Planeación

Identificación del riesgo:

- Se debe seleccionar el nombre del proceso(lista desplegable)
- Se debe hacer una descripción breve del riesgo
- Se debe determinar las causas
- Se debe seleccionar las consecuencias (lista desplegable)
- Se debe determinar el tipo de riesgo (lista desplegable)

Riesgo Inherente:

- Se debe seleccionar el valor de la probabilidad (lista desplegable)
- Se debe seleccionar el valor de la Impacto (lista desplegable)
- El nivel de riesgo se calcula automáticamente
- Se debe seleccionar la zona de riesgo (lista desplegable)

Evaluación de controles

- Se debe diligenciar la descripción del control incluyendo: Quien lo hace, cada cuanto lo hace, cuando lo hace, que se hace, como se hace y la evidencia que queda de la ejecución del control.
- Se debe seleccionar si el control es preventivo o correctivo (lista desplegable)
- Se deben responder las preguntas de la hoja "controles" y esta automáticamente calcula el valor de la calificación.

Riesgo residual

- Se debe seleccionar el valor de la probabilidad (lista desplegable)
- Se debe seleccionar el valor de la Impacto (lista desplegable)
- El nivel de riesgo se calcula automáticamente
- Se debe seleccionar la zona de riesgo (lista desplegable)

Plan de respuesta

- Se debe seleccionar la medida de tratamiento(lista desplegable)
- Se debe establecer la acción o acciones a tomar frente al riesgo cantidad y periodicidad (1 diaria, 3 semanal, 2 mensual, 1 bimensual, 1 trimestral, 1 semestral etc.)
- Se debe establecer una fecha de Inicio de las acciones o actividades(Esta fecha hace referencia a la fecha en la cual se desarrollará por primera vez la actividad)
- Se debe establecer un periodo durante el cual se le dará cumplimiento a las acciones o actividades en meses y preferiblemente dentro de la vigencia actual.
- Se debe establecer un responsable frente a la ejecución de las acciones o actividades

3.4 Valoración del Riesgo de Corrupción

Para los riesgos de corrupción fue necesario desarrollar la etapa de valoración del riesgo en un capitulo independiente, ya que en esta existen algunas diferencias en la metodología entre los riesgos de gestión y los de corrupción.

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[7]. La posibilidad no implica la materialización del riesgo.

Los componentes básicos de un riesgo de corrupción son:

- La existencia de una acción u omisión
- El uso del Poder
- Desviar la gestión de lo público
- Beneficio particular

[7] (Guía para la gestión del riesgo de corrupción. Presidencia de la República, 2015)

Al igual que los riesgos de Gestión, para los riesgos de Corrupción el análisis del riesgo implica una combinación del análisis del impacto y la probabilidad. Sin embargo para los riesgos de corrupción el impacto se valora de manera diferente, ya que solo contempla 3 niveles de impacto.

3.4.1 Análisis del riesgo de corrupción

Esta etapa tiene como principal objetivo determinar la probabilidad de materialización del riesgo y sus consecuencias o impacto y su medición se realiza de acuerdo a los parámetros establecidos por la Guía de gestión de riesgos de corrupción, con el fin de establecer la zona de riesgo inicial o riesgo inherente.

a. Calificación de la probabilidad

La probabilidad es la posibilidad de ocurrencia de un evento de riesgo y se mide según su frecuencia, es decir el número de veces en que pudo haberse presentado el evento en un periodo determinado. La probabilidad de se califica de acuerdo a los siguientes parámetros:

Nivel	Descriptor	Descripción	Frecuencia
5	Casi seguro	Se espera que el evento ocurra en la mayoría de las circunstancias	Existe la posibilidad que se haya presentado más de una vez en el Último año.
4	Probable	Es viable que el evento ocurra en la mayoría de las circunstancias	Existe la posibilidad que se haya presentado una vez en el último año.
3	Posible	El evento podrá ocurrir en algún momento	Existe la posibilidad que se haya presentado una vez en los últimos 2 años.
2	Improbable	El evento puede ocurrir en algún momento	Existe la posibilidad que se haya presentado una vez en los últimos 5 años
1	Rara vez	El evento puede ocurrir solo en circunstancias excepcionales (Poco comunes o anormales).	Existe la posibilidad que no se haya presentado en los últimos 5 años.

Fuente Oficina de Planeación

b. Calificación del impacto

El impacto es la consecuencia o efecto que puede generar la materialización del riesgo. Los riesgos de corrupción siempre generan un impacto negativo para las Entidades; por esa razón para este tipo de riesgos no aplican las categorías de calificación (1) insignificante o (2) menor señalados en la Guía de Función Pública para los riesgos de Gestión.

Para los riesgos de corrupción el Impacto se califica de acuerdo a los siguientes parámetros:

- **Moderado:** Genera medianas consecuencias sobre la entidad.
- **Mayor:** Genera altas consecuencias sobre la entidad.
- **Catastrófico:** Genera consecuencias desastrosas para la entidad.

Para determinar la calificación del impacto se debe responder "si = 1" o "no = 0" a las preguntas que se encuentra en el formato para el levantamiento del mapa de riesgos de corrupción de la unidad en la hoja "Impacto".

Fuente Oficina de Planeación

El resultado de las preguntas se evaluará así:

Calificación del Riesgo de Corrupción - Impacto[8]

Calificación de Riesgo de Corrupción Impacto		
Respuestas	**Descripción**	**Nivel**
1-5	Moderado	5
6-11	Mayor	10
12-18	Castrófico	20

c. Determinación del riesgo inherente

Luego de obtenida el resultado de la calificación de la probabilidad y el impacto, se realiza la multiplicación del puntaje de la probabilidad por el puntaje del impacto para obtener el riesgo inherente, este resultado se ubica en una de las cuatro (4) zonas de riesgo que a continuación se describen:

Resultados de la calificación del Riesgo de Corrupción[9]

Resultados de la calificación del Riesgo de Corrupción				
Probabilidad	**Puntaje**	**Zonas de riesgo de corrupción**		
Casi seguro	5	25 Moderada	50 Alta	100 Extrema
Probable	4	20 Moderada	40 Alta	80 Extrema
Posible	3	15 Moderada	30 Alta	60 Extrema
Improbable	2	10 Baja	20 Moderada	40 Alta
Rara vez	1	5 Baja	10 Baja	20 Moderada
Impacto		Moderado	Mayor	Catastrófico
Puntaje		5	10	20

PROBABILIDAD

IMPACTO

[8] (Guía para la gestión del riesgo de corrupción. Presidencia de la República, 2015)
[9] (Guía para la gestión del riesgo de corrupción. Presidencia de la República, 2015)

Zona de Riesgo Baja: De 5 a 10 puntos.

- Probabilidad: Rara vez o improbable.
- Impacto: Moderado y Mayor.
- Tratamiento: Los riesgos de corrupción de las zonas baja se encuentran en un nivel que puede eliminarse o reducirse fácilmente con los controles establecidos en la entidad.

Zona de Riesgo Moderada: De 15 - 25 puntos.

- Probabilidad: Rara vez, Improbable, Posible, Probable y Casi Seguro.
- Impacto: Moderado, Mayor y Catastrófico.
- Tratamiento: Deben tomarse las medidas necesarias para llevar los riesgos a la Zona de Riesgo Baja o eliminarlo.

Zona de Riesgo Alta: De 30 - 50 puntos.

- Probabilidad: Improbable, Posible, Probable y Casi Seguro.
- Impacto: Mayor y Catastrófico.
- Tratamiento: Deben tomarse las medidas necesarias para llevar los riesgos a la Zona de Riesgo Moderada, Baja o eliminarlo.

Zona de Riesgo Extrema: De 60 - 100 puntos.

- Probabilidad: Posible, Probable y Casi Seguro.
- Impacto: Catastrófico.
- Tratamiento: Los riesgos de corrupción de la Zona de Riesgo Extrema requieren de un tratamiento prioritario. Se deben implementar los controles orientados a reducir la posibilidad de ocurrencia del riesgo o disminuir el impacto de sus efectos y tomar las medidas de protección.

3.4.2 Evaluación del riesgo de corrupción

En esta etapa se evalúan los controles que se encuentran establecidos para cada riesgo y de acuerdo al puntaje obtenido, se reduce la zona de riesgo en la que se encuentra ubicado el riesgo inherente obteniendo como resultado el riesgo residual.

a. Evaluación de controles

Para la evaluación de los controles se deben determinar los siguientes factores:

- Determinar la naturaleza de los controles: Preventivos o correctivos.
- Determinar si los controles están documentados
- Determinar las clases de controles: Manuales o automáticos

Para la realización de esta evaluación se ha determinado el siguiente cuestionario, el cual está incluido en el formato para el levantamiento del mapa de riesgos de corrupción de la unidad en la hoja "Controles".

Evaluación controles del Riesgo de Corrupción

De 0 a 50 = 0 De 51 a 75=1 De 76 a 100 = 2						
RIESGO 1						
0		Control 1.1	Control 1.2	Control 1.3	Control 1.4	Control 1.5
		0	0	0	0	0
¿El control previene la materialización del riesgo (afecta probabilidad- Preventivo), ¿El control permite enfrentar la situación en caso de materialización, (afecta impacto - Correctivo)?		0	0	0	0	0
Calificaciones	VALOR	SI	SI	SI	SI	SI
¿Existen manuales, instructivos o procedimientos para el manejo del control?	15					
¿Está(n) definido(s) el(los) responsable(s) de la ejecución del control y del seguimiento?	5					
¿El control es automático?	15					
¿El control es manual?	10					
¿La frecuencia de ejecución del control y seguimiento es adecuada?	15					
¿Se cuenta con evidencias de la ejecución y seguimiento del control?	10					
¿En el tiempo que lleva la herramienta ha demostrado ser efectiva?	30					
TOTAL	100	0	0	0	0	0

Fuente Oficina de Planeación

b. Determinación del Riesgo Residual

Se comparan los resultados obtenidos del riesgo inherente con los controles establecidos, para Establecer la zona del riesgo final o riesgo residual. Se califica de acuerdo con la siguiente tabla.

Calificación de los Controles[10]

Calificación de los controles	Puntaje a disminuir
De 0 a 50	0
De 51 a 75	1
De 76 a 100	2

Con la calificación obtenida se realiza un desplazamiento en la matriz, así:

- Si el control es correctivo afecta el impacto se disminuye a la izquierda.
- Si el control es preventivo afecta la probabilidad se disminuye hacia abajo.

[10] (Guía para la gestión del riesgo de corrupción. Presidencia de la República, 2015)

Si el control no genera ningún efecto en la probabilidad o impacto, debe ser eliminado o en su defecto debe generarse una acción en el plan de respuesta que permita en el futuro mejorar su calificación.

Nota:

*Si existen más de dos controles del mismo tipo el valor de la disminución será un promedio de la calificación de los controles.

Resultados de la calificación de los controles[11]

Resultados de la calificación del Riesgo de Corrupción				
Probabilidad	**Nivel**	**Zonas de riesgo de corrupción**		
Casi seguro	5	←		
Probable	4	←		
Posible	3	←		
Improbable	2	←		
Rara vez	1	←		
Impacto		Moderado	Mayor	Catastrófico
NIvel		3	4	5

Si afecta el impacto se desplaza a la izquierda

IMPACTO

PROBABILIDAD

Resultados de la calificación del Riesgo de Corrupción				
Probabilidad	**Nivel**	**Zonas de riesgo de corrupción**		
Casi seguro	5			
Probable	4			
Posible	3			
Improbable	2			
Rara vez	1	↓	↓	↓
Impacto		Moderado	Mayor	Catastrófico
NIvel		3	4	5

Si afecta la probabilidad se desplaza hacia abajo.

+

3.4.3 Mapa de riesgos de corrupción

La información sobre los resultados de las etapas de Identificación, valoración y seguimiento, así como la información sobre el plan de respuesta, se registran el formato para el levantamiento de mapa de riesgos de corrupción del proceso de la siguiente manera:

[11] (Guía para la gestión del riesgo de corrupción. Presidencia de la República, 2015)

Identificación del riesgo:

- Se debe seleccionar el nombre del proceso(lista desplegable)
- Se debe hacer una descripción breve del riesgo
- Se debe determinar las causas
- Se debe seleccionar las consecuencias (lista desplegable)
- Tipo de riesgo predeterminado como riesgo de corrupción

Riesgo Inherente:

- Se debe registra el valor de la probabilidad
- Se debe registra el valor del impacto de acuerdo al resultado de la hoja "Impacto".
- El nivel de riesgo se calcula automáticamente
- La zona de riesgo se muestra automáticamente

Evaluación de controles

- Se debe diligenciar la descripción del control incluyendo: Quien lo hace, cada cuanto lo hace, cuando lo hace, que se hace, como se hace y la evidencia que queda de la ejecución del control.
- Se debe seleccionar si el control es preventivo o correctivo (lista desplegable)
- Se deben responder las preguntas de la hoja "controles" y esta automáticamente calcula el valor de la calificación.

Riesgo Residual

- Se debe seleccionar el valor de la probabilidad o Impacto, luego de la disminución.
- El nivel de riesgo se calcula automáticamente
- La zona de riesgo se muestra automáticamente

Plan de respuesta

- Se debe seleccionar la medida de tratamiento(lista desplegable)
- Se debe establecer la acción o acciones a tomar frente al riesgo y la periodicidad con la cual se desarrollarán (diaria, semanal, mensual, bimensual, trimestral, semestral etc.)
- Se debe establecer una fecha de Inicio de las acciones o actividades(Esta fecha hace referencia a la fecha en la cual se desarrollará por primera vez la actividad)
- Se debe establecer un periodo durante el cual se le dará cumplimiento a las acciones o actividades en meses y preferiblemente dentro de la vigencia actual.
- Se debe establecer un responsable frente a la ejecución de las acciones o actividades

Mapa de riesgos de corrupción[12]

FORMATO PARA EL LEVANTAMIENTO DEL MAPA DE RIESGOS DE CORRUPCIÓN DE LA UNIDAD
PROCESO DE DIRECCIONAMIENTO ESTRATÉGICO
Procedimiento de Administración de Riesgos Institucionales y de Proceso

IDENTIFICACION						RIESGO INHERENTE				CONTROLES			RIESGO RESIDUAL				PLAN DE RESPUESTA AL RIESGO (PROCESO)						
No	Proceso	Riesgo	Causas	Consecuencias	Tipo de riesgo	Probabilidad	Impacto	Nivel Riesgo	Zona de Riesgo	Descripción	Correctivo-Impacto Preventivo-Probab.	Calificación De 0 a 50 = 0 De 51 a 75=1 De 76 a 100 = 2	Probabilidad	Impacto	Nivel Riesgo	Zona de Riesgo	Medida de Tratamiento	Acción o Actividades	Meta	Fecha de Inicio	Duración	Responsable	P
1					Corrupción			0	0			0			0	0							
												0											
												0											
												0											
			Otros:									0											
												0											

4. PLAN DE RESPUESTA

Una vez culminada la etapa de valoración del riesgo es necesario establecer un plan de respuesta al riesgo que incluye establecer la medida de tratamiento, las acciones para el manejo de riesgos, la meta, la fecha de inicio, la periodicidad y la duración de la acción y el responsable de ejecutarla.

4.1 Medidas de Tratamiento

- Evitar el riesgo: Esta medida se implica tomar las medidas encaminadas a prevenir su materialización. Esta siempre debería ser la primera alternativa a considerar, se logra cuando al interior de los procesos se generan cambios sustanciales por mejoramiento, rediseño o eliminación, resultado de unos adecuados controles y acciones emprendidas. Para reducir el riesgo se pueden tomar medidas como control de calidad, mantenimiento preventivo de los equipos, desarrollo tecnológico, entre otros

- Reducir el riesgo: Esta medida implica tomar medidas encaminadas a disminuir tanto la probabilidad como el impacto. La reducción del riesgo es probablemente el método más sencillo y económico para superar las debilidades antes de aplicar medidas más costosas y difíciles. Para reducir el riesgo se pueden tomar medidas como la optimización de los procedimientos y la implementación de controles.

- Compartir o transferir el riesgo: Esta medida implica reducir su efecto a través del traspaso de las pérdidas a otras organizaciones o a través de otros medios que permiten distribuir una porción del riesgo Para transferir o compartir el riesgo se pueden medidas como adquirir seguros o contratos a riesgo compartido.

- Asumir el riesgo Luego de que el riesgo ha sido reducido o transferido puede quedar un riesgo residual bajo, en este caso simplemente acepta la pérdida residual probable y elabora planes de contingencia para su manejo.

[12] (Guía para la gestión del riesgo de corrupción. Presidencia de la República, 2015)

4.2 Acciones o actividades

Estas acciones o actividades deben estar encaminadas a reducir o eliminar las causas originadoras del riesgo y deben planearse de tal manera que puedan convertirse en el futuro en controles que puedan reducir el nivel de riesgo. Estas acciones deben ser concretas y verificables.

4.3 Fecha de inicio, periodicidad, periodo y responsable

Se debe establecer la fecha en que iniciará la acción la periodicidad con que será realizada (diaria, semanal, mensual, bimensual, trimestral, semestral etc.). Adicionalmente se debe establecer el tiempo durante el cual se llevará a cabo la actividad o actividades, este debe ser suficiente para demostrar su efectividad y en lo posible debe establecer dentro de la vigencia en la cual se realice la actualización del mapa. Finalmente se debe establecer un responsable frente cada actividad del plan de respuesta, esta responsabilidad se puede asignar a un cargo; sin embargo para los riesgos de corrupción si se hace necesario que esta responsabilidad recaiga en el funcionario o contratista que realice la labor.

5. Monitoreo y revisión

Esta etapa permite determinar la necesidad de modificar, actualizar o mantener en las mismas condiciones los factores de riesgo, así como su identificación, análisis y valoración[13].

5.1 Revisión y actualización del Mapa de riesgos

Los líderes de los procesos en conjunto con sus equipos deben revisar y actualizar periódicamente el documento del Mapa con el acompañamiento Equipo Nacional de Gestión y Seguimiento de Riesgos, crisis y comunicaciones estratégicas y hacer los ajustes pertinentes. Su importancia radica en la necesidad de monitorear permanentemente la gestión del riesgo, la efectividad de los controles establecidos y la identificación de nuevos riesgos.

En esta fase se debe:

- Asegurar que los controles son eficaces y eficientes.
- Obtener información adicional que permita mejorar la valoración del riesgo.
- Analizar y aprender lecciones a partir de los eventos, los cambios, las tendencias, los éxitos y los fracasos.
- Detectar cambios en el contexto interno y externo.
- Identificar riesgos nuevos riesgos en el proceso.
- Reportar y tomar acciones sobre los riesgos materializados

Para este monitoreo, se deberá tener en cuenta:

[13] (Guía para la gestión del riesgo de corrupción. Presidencia de la República, 2015)

- Riesgos materializados (ver Formato de monitoreo de riesgos de gestión y de corrupción).
- Observaciones, investigaciones disciplinarias, penales, fiscales, o de entes reguladores,
- Hallazgos por parte de la Oficina de Control Interno.
- Cambios importantes en el entorno que den lugar a nuevos riesgos.

5.2 Monitoreo Materialización de los riesgos

El líder del proceso en conjunto con su equipo, es el responsable de monitorear permanentemente la materialización de riesgos y repórtala al Equipo Nacional de Gestión y Seguimiento de Riesgos, crisis y comunicaciones estratégicas. Este monitoreo se registrará en el Formato de monitoreo de riesgos institucionales.

En caso de materializarse un riesgo deberán tomarse las siguientes acciones:

- Informar al Equipo Nacional de Gestión y Seguimiento de Riesgos, crisis y comunicaciones estratégicas.
- Realizar la corrección, con respecto a los efectos del riesgo.
- Generar la acción correctiva correspondiente.
- Realizar Actualización al mapa de riegos del proceso, en particular a las causas, riesgos y controles.

5.3 Periodicidad

El Monitoreo del Mapa de Riesgos por parte de los Procesos y con el acompañamiento Equipo Nacional de Gestión y Seguimiento de Riesgos, crisis y comunicaciones estratégicas se realizará tres (3) veces al año en las siguientes fechas:

- Primer Monitoreo: Con corte al 31 de febrero.
- Segundo Monitoreo: Con corte al 31 de Junio.
- Tercer seguimiento: Con corte al 30 de Octubre.

5.4 Actualización del mapa de riesgo

De acuerdo con el resultado de la revisión y monitoreo realizado, se verificará si los mapas de riesgos deben ser actualizados o si se mantienen bajo las mismas condiciones en cuanto a factores de riesgo, identificación, análisis y valoración del riesgo. No obstante, los riesgos deben ser flexibles y permitir cambios en cualquier momento. Los aspectos analizados en la revisión y monitoreo, deben ser considerados para posibles ajustes o cambios sobre los lineamientos establecidos en la política de riesgos institucional, para fortalecer la administración del riesgo de la Unidad.

6. Seguimiento

La Oficina de Control Interno debe adelantar seguimiento a Mapa de Riesgos Institucional. En este sentido es necesario que en sus procesos de auditoría interna analice las causas, los riesgos y la efectividad de los controles incorporados en el Mapa de Riesgos de Corrupción.

El Jefe de Control Interno o quien haga sus veces, es el encargado de verificar y evaluar la elaboración, seguimiento y control del Mapa de Riesgos Institucional.

6.1 Aspectos relevantes en la realización del Seguimiento

En la realización del seguimiento se deben evaluar los siguientes aspectos:

- Revisión de las causas
- Revisión de los riesgos y su plan de respuesta.
- Revisión de los controles y su efectividad, le apunten al riesgo y estén funcionando en forma oportuna y efectiva.
- Revisión al cumplimiento de la tarea de monitoreo a la materialización de los riesgos.

6.2 Seguimiento al monitoreo de la materialización de Riesgos de Corrupción

En el evento de materializarse un riesgo de corrupción la Entidad debe emprender las siguientes acciones:

- Informar al Grupo nacional de manejo de crisis
- Revisar el Mapa de Riesgos de Corrupción, en particular las causas, riesgos y controles.
- Verificar si se tomaron las acciones y se actualizó el Mapa de Riesgos de Corrupción.
- Realizar un monitoreo permanente.

6.3 Periodicidad

El seguimiento del Mapa de Riesgos se realizará tres (3) veces al año en las siguientes fechas:

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

6.4 Resultados del seguimiento

El seguimiento adelantado por la Oficina de Control Interno se deberá publicar en la página web de la entidad o en lugar de fácil acceso al ciudadano.

El seguimiento adelantado por la Oficina de Control Interno a los mapas de riesgos debe ser retroalimentado a los líderes de los procesos identificando las falencias y puntos a revisar para que estos a su vez tomen acciones y den respuesta a dichas observaciones.

La Alta dirección o su representante debe analizar estratégicamente los resultados e informes de seguimiento a los mapas de riesgos de la entidad, con el fin de tomar las decisiones requeridas para la mejora de la gestión del riesgo en la entidad o para actualizar la política de administración del Riesgo.

7. Divulgación, comunicación estratégica y consulta

La NTC ISO 31000 define la comunicación y consulta como un proceso continuo y reiterativo que una organización lleva a cabo para suministrar, compartir y obtener información e involucrarse en un diálogo con las partes interesadas con respecto a la Administración del Riesgo.

La comunicación y consulta son necesarias en cada una de las etapas de la Administración del Riesgo, el cual implica un diálogo con las partes interesadas, con esfuerzos centrados más en la consulta que en la forma de flujo de información desde quien toma la decisión hasta otras partes interesadas. Este análisis debe garantizar que se tienen en cuenta las necesidades de los usuarios o partes interesadas, de modo tal que los riesgos identificados, permitan encontrar puntos críticos para mejorar la prestación del servicio[14].

Para el desarrollo de esta etapa, se harán sesiones de trabajo que el equipo operativo del SIG Equipo Nacional de Gestión y Seguimiento de Riesgos, crisis y comunicaciones estratégicas y al interior de cada proceso, a través de discusiones técnicas en la que identificarán, analizarán, valorarán y definirán acciones que alimenten el plan de respuesta al riesgo. Discusiones técnicas que se llevarán a cabo con equipos multidisciplinarios que tengan amplio conocimiento y experiencia en el quehacer de cada proceso, con el fin de mantener una comunicación y consulta fluida que enriquezca el ejercicio de la Administración del Riesgo en la Unidad.

La divulgación y consulta de los mapas de riesgos se realizará en la Intranet y la página web de la Unidad. Adicionalmente se realizarán socializaciones de los cambios o actualizaciones de los documentos asociados a la Metodología de riesgos, incluyendo la Metodología de administración de riesgos Institucionales, el procedimiento de administración de riesgos y los mapas de riesgos.

[14] (Guía para la Administración del riesgo. Departamento Administrativo de la Función Pública, 2015)

Finalmente se establecerán unos protocolos y manuales para el manejo de riesgos, crisis y comunicaciones estratégicos los cuales serán gestionados por el Grupo nacional de manejo de crisis.

8. Roles y Responsabilidades

La entidad ha definido la siguiente matriz de roles y responsabilidades para las etapas de la aplicación de la metodología de Administración de riesgos:

Matriz de roles y responsabilidades

Pasos Metodologia	Direccionamiento Estrategico	Líder del Proceso	Enlaces SIG	Servidores (s) responsable (s) de la actividad o procedimiento	Oficina de Control Interno	Oficina de Planeación o quien haga sus veces
Política para la administración del riesgo.	Determinar los lineamientos para la administración del riesgo en la entidad. Dichos lineamientos deben incluir los aspectos necesarios para la identificación y mitigación de los riesgos.	Dar a conocer a su equipo de trabajo los lineamientos determinados en la política institucional de riesgos	Conocer, apropiar y dar a conocer la política institucional de riesgos.	Conocer y apropiar la política institucional de riesgos.	NA	Difundir la política institucional de riesgos a lo largo de toda la organización.
Establecimiento del Contexto	Realizar el analisis de contexto estrategico de la entidad para facilitar la identificación de riesgos a los procesos.	Analizar el contexto del proceso conjunto con su equipo de trabajo.	Participar en el análisis de contexto del proceso donde interactúa e impulsar la participacion de los otros Servidores de su proceso.	Participar en el análisis de contexto del proceso donde interactúa.	NA	Acompañar a los procesos levantamiento de los mapas de riesgo en cada una de sus etapas. Consolidar el plan anticorrupción y de atención al ciudadano, donde están incluidos los mapas de riesgos relacionados con posibles actos de corrupción.
Identificación del Riesgo	NA	Realizar la identificación de causas y consecuencias de acuerdo al contexto e identificar los riesgos para su proceso.	Participar en la identificación de causas de acuerdo al contexto e identificar los riesgos para su proceso e impulsar la participacion de los otros Servidores de su proceso.	Participar en la identificación de causas de acuerdo al contexto e identificar los riesgos para su proceso	NA	Acompañar y asesorar a los procesos en la etapa de identificación.

Pasos Metodologia	Direccionamiento Estrategico	Líder del Proceso	Enlaces SIG	Servidores (s) responsable (s) de la actividad o procedimiento	Oficina de Control Interno	Oficina de Planeación o quien haga sus veces
Análisis y Valoración del Riesgo	NA	Analizar la probabilidad e impacto de los riesgos identificados para el proceso. Establecer los controles idóneos que permitan administrar los riesgos identificados.	Participar en el analisis de probabilidad e impacto de los riesgos identificados para el proceso, ayudar a identificar los controles e impulsar la participacion de los otros Servidores de su proceso.	Participar en el analisis de probabilidad e impacto de los riesgos identificados para el proceso Participar en el analisis de los controles idóneos que permitan administrar los riesgos identificados	NA	Acompañar y asesorar a los procesos en la etapa de Valoración
Aprobación Mapa de riesgos Institucional	Aprobar mapa de riesgos Institucional	Aprobar mapa de riesgos de gestión y de riesgos de corrupción del proceso	NA	NA	NA	Coordinar la aprobación de los mapas de riesgos de los procesos para su aprobación. Consolidar y remitir a la Alta Dirección el mapa de riesgos institucional para su aprobación.
Planes de Respuesta	NA	Asegurar la ejecución de los controles y de las acciones del Plan de respuesta a los riesgos de su proceso.	Ejecución de los controles a su cargo, Ejecucion de las acciones del Plan de respuesta que tenga a su cargo	Ejecución de los controles a su cargo, Ejecucion de las acciones del Plan de respuesta que tenga a su cargo	Realizar seguimiento al Plan de respuesta y Acciones relacionadas	Realizar asesoria en la formulación de los Planes de respuesta
Monitoreo	NA	Atender todos los requerimientos de la oficina de planeacion con respecto a los Mapas de riesgos de gestión y de corrupción y Metodología de Administración de riesgos de la unidad. Participar en la Mesas de trabajo para la revisión y actualización de los riesgos. Realizar el monitoreo de la materializacion de los riesgos del proceso y tomar acciones frente a los resultados.	Atender todos los requerimientos de la oficina de planeacion con respecto a los Mapas de riesgos de gestion y de corrupcion, monitoreo a la materializacion de riesgo y Metodologia de Administracion de riesgos de la unidad. Participar en la Mesas de trabajo para la revision y actualización de los riesgos. Realizar el monitoreo de la materializacion de los riesgos del proceso y tomar acciones.	Tomar la responsabilidad frente al seguimiento de los controles que están a su cargo de acuerdo a las funciones que realiza y realizarlo en los tiempos estipulados	NA	Realizar Monitoreo al mapa de riesgos del proceso y al monitoreo la materializacion del riesgo.

Pasos Metodologia	Direccionamiento Estrategico	Líder del Proceso	Enlaces SIG	Servidores (s) responsable (s) de la actividad o procedimiento	Oficina de Control Interno	Oficina de Planeación o quien haga sus veces
Seguimiento	Realizar el seguimiento correspondiente al mapa de riesgos del proceso de Direccionamiento Estratégico. Analizar estratégicamente los resultados e informes de seguimiento a los mapas de riesgos de la entidad, con el fin de tomar las decisiones requeridas para la mejora de la gestión del riesgo en la entidad o para actualizar la política de Administración del Riesgo.	Atender todos los requerimientos de la oficina de control Interno con respecto a los Mapas de riesgos de gestion y de corrupcion, planes de respuesta y monitoreo a la materializacion de riesgo.	Atender todos los requerimientos de la oficina de control Interno con respecto a los Mapas de riesgos de gestion y de corrupcion, planes de respuesta y monitoreo a la materializacion de riesgo.	Atender todos los requerimientos de la oficina de control Interno con respecto a los Mapas de riesgos de gestion y de corrupcion, planes de respuesta y monitoreo a la materializacion de riesgo.	Adelantar seguimiento al mapa de riesgos de corrupción y al mapa de riesgos de gestión. Analizar el diseño e idoneidad de los controles, determinando si son o no adecuados para prevenir o mitigar los riesgos de los procesos y determinar la efectividad de los controles. Realizar seguimiento al los planes de respuesta, a la ejecución de las acciones, al nivel de avance y materialización del riesgo.	NA
Comunicación y Consulta	Disponer del tiempo y recursos necesarios para dar a conocer a todos los funcionarios la política institucional de riesgos y la metodología para la construcción del mapa de riesgos de gestion y el mapa de riesgos de corrupcion.	Debe participar en los procesos de aprendizaje que se programen y facilitar la asistencia de los funcionarios de su equipo de trabajo.	Como representantes y facilitadores de cada proceso deben apropiar los conocimientos necesarios frente a la metodología de administración del riesgo, con el fin de realimentar a los miembros de sus equipos o procesos dentro de la entidad.	Participar en los procesos de aprendizaje programados	NA	Coordinar el proceso de comunicación y consulta, generando espacios para la capacitación o acompañamiento técnico a los funcionarios sobre la metodología de administración de riesgos.

6. DOCUMENTOS DE REFERENCIA

DEPARTAMENTO ADMINISTRATIVO DE LA FUNCION PUBLICA, Decreto 0943 del 21 mayo de 2014, Por el cual se actualiza el Modelo Estándar de Control Interno MECI.

DEPARTAMENTO ADMINISTRATIVO DE LA FUNCION PÚBLICA Guía de administración de riesgos, Bogotá: Cuarta edición septiembre de 2015

ICONTEC Gestión de riesgos: Norma técnica colombiana NTC ISO 31000, Bogotá: Febrero 16 de 2011

ICONTEC Guía técnica colombiana: Gestión de riesgos - Vocabulario GTC 137, Bogotá: Febrero 16 2011

ICONTEC Comunicación y consulta acerca del riesgo HB327:2010, Bogotá: Octubre de 2011

SECRETARIA DE TRANSPARENCIA, Guía para la gestión del riesgo de corrupción, 2015

H. ANEXOS

ANEXO 1

Riesgo de seguridad personal – riesgos personales

En el presente anexo se explicará la etapa del análisis del riesgo para los riesgos de seguridad, ya que existen algunos parámetros diferentes en la metodología propuesta por Departamento de Seguridad de las Naciones Unidas – UNDSS con base en la cual estamos trabajando este tipo de riesgos. Estos riesgos serán identificados en la Unidad como parte de un trabajo estratégico realizado por la dirección y serán parte del mapa de riesgos del proceso de Direccionamiento estratégico.

Los riesgos de seguridad personal son todos los riesgos asociados a todas aquellas amenazas que podrían afectar al personal, activos u operaciones de la Unidad.

- Personal:
- Activos:
- Operaciones:

Análisis del riesgo de seguridad personal

Al igual que los riesgos de Gestión y corrupción para los riesgos de seguridad personal el análisis del riesgo implica una combinación del análisis del impacto y la probabilidad. Sin embargo las tablas con las cuales se valora la probabilidad y el impacto son diferentes ya que determinan un impacto en tres niveles: al personal, activos u operaciones.

Esta etapa tiene como principal objetivo determinar la probabilidad de materialización del riesgo y sus consecuencias o impacto y su medición se realiza de acuerdo a los parámetros establecidos por el Departamento de Seguridad de las Naciones Unidas – UNDSS.

c. Calificación de la probabilidad

La probabilidad es la posibilidad de ocurrencia de un evento de riesgo. La probabilidad de se califica de acuerdo a los siguientes parámetros:

Descripción	Valor	Descripción		Valor
Intención, (I)		Circunstancias, (C)	Tendencia, (T)	
No existe información que sugiera que el evento pudiera causar algún impacto negativo en la Unidad	Minimo, 0	Bajo ninguna circunstancia se espera que el evento impacte a la Unidad	No se conoce de ninguna tendencia, el evento no ocurrio durante mucho años consecutivamente	Minimo, 0
Información general disponible, limitada, que sugiere que el evento podria impactar a la Unidad	Bajo, 1	Se espera que el evento impacte a la Unidad en circunstancias excepcionales	Rara tendencia de eventos; un acontecimiento en muchos años consecutivos	Bajo, 1
Informacion general consistente , indicando que el evento podría impactar a la Unidad	Medio, 5	Se espera que el evento impacte a la Unidad en algunas circunstancias	Tendencia periodica, algunos sucesos en muchos años consecutivos	Medio, 2
Informacion general consistente y alguna información especifica que indique que el evento impactará a la Unidad	Alto, 30	Se espera que el evento impacte a la Unidad en la mayoria de circunstancias	Tendencia Frecuente, hechos unicos ocurridos en muchos años de manera consecutiva	Alto, 5
Informacion general y especifica , confirmada que se espera que el evento impacte a la Unidad.	Maximo, 40	Se espera que el evento impactará a la Unidad en la mayoria de circunstancias	Tendencia persistente, multiples ocurrencias anuales, durante muchos años y de manera consecutiva	Maximo, 10

Fuente Oficina de Planeación

De acuerdo a los resultados obtenidos la probabilidad se calificará de la siguiente manera:

Valor numérico de la probabilidad	Probabilidad	Nivel
<1	Muy improbable	1
2-5	Improbable	2
6-18	Moderadamente Probable	3
19-49	Probable	4
>50	Muy probable	5

d. Calificación del impacto

El impacto es la consecuencia o efecto que puede generar la materialización del riesgo. Para los riesgos de seguridad personal el Impacto se califica de acuerdo a los siguientes aspectos:

- **Personal:** Se conoce como personal al conjunto de las personas que trabajan en un mismo organismo, empresa o entidad.
- **Activos:** Son los bienes, derechos y otros recursos controlados económicamente por la Entidad
- **Operaciones:** Ejecuciones o maniobras metódicas y sistemáticas sobre cuerpos, números, datos, etcétera, para lograr un determinado fin.

Para determinar la calificación del impacto se debe calificar el Impacto de acuerdo a la siguiente parámetros:

Nivel	Impacto	Personal	Activos	Operaciones
1	Insignificante	Sin Lesiones	Perdidas y daños minimos a bienes	No hay retrasos en programas
2	Menor	Lesiones Menores	Posibles perdidas o daños a bienes	Atrasos limitados en programas
3	Moderado	Lesiones que no ponen en peligro la vida. Alto nivel de stress	Algunos daños y perdidas de bienes	Algun retraso en los programas
4	Severo	Muerte o Lesiones graves	Perdidas significativas de bienes	Atrasos mayores en los programas
5	Critico	Incidente de bajas masivas	Perdidas mayores o destruccion de bienes	Cancelación de los programas

Fuente Oficina de Planeación

c. Determinación del riesgo inherente

Luego de obtenida el resultado se ubica en la Matriz de análisis de riesgo la probabilidad y el impacto, se realiza la multiplicación del puntaje de la probabilidad por el puntaje del impacto para obtener el riesgo inherente, este resultado se ubica en una de las zonas de riesgo que a continuación se describen:

Resultados de la calificación del Riesgo

NIVEL		Impacto				
		Insignificante (1)	Menor (2)	Moderado (3)	Severo (4)	Critico (5)
Probabilidad	Muy probable (5)	bajo 5	medio 10	Alto 15	Muy Alto 20	Inaceptable 25
	Probable (4)	bajo 4	medio 8	Alto 12	Alto 16	Muy Alto 20
	Moderadamente Probable (3	muy bajo 3	bajo 6	medio 9	Alto 12	Alto 15
	Improbable (2)	muy bajo 2	bajo 4	bajo 6	medio 8	medio 10
	Muy improbable (1)	nulo 1	muy bajo 2	muy bajo 3	bajo 4	bajo 5

En el mapa de riesgos se ubicará el nivel de riesgos de acuerdo a la siguiente clasificación:

Zona de Riesgo baja (Nulo, muy bajo y bajo): De 1 - 6 puntos.
Zona de Riesgo Moderada (medio): De 8 - 10 puntos.
Zona de Riesgo Alta (Alto): De 12 - 16 puntos.
Zona de Riesgo Extrema (Muy Alto, Inaceptable): De 20 - 25 puntos.

Para los riesgo de seguridad personal las etapas de Evaluación del riesgo y Monitoreo y revisión se desarrollarán de la misma manera como se hace para el resto de riesgos de gestión.

ANEXO 2

Identificación de peligros y riesgos en el desarrollo de las actividades laborales - Seguridad y salud en el trabajo

Como parte del trabajo de identificación de riesgos el proceso de talento humano realiza la identificación de peligros y evaluación de riesgos en el desarrollo de las actividades laborales de acuerdo a los parámetros establecidos en el presente anexo, cuyos resultados se consignan en la "Matriz de identificación de peligros, valoración de riesgos y determinación de controles", el cual sirve como insumo para identificar los riesgos de Seguridad y salud en el trabajo que harán parte de la Matriz de riesgos institucionales de la Unidad.

a. Levantamiento de información para la identificación de peligros

Para realizar la identificación de peligros y evaluación de riesgos se ha diseñado la "Matriz de identificación de peligros, valoración de riesgos y determinación de controles" aplicable a toda la organización con el fin de asegurar una acción proactiva y no reactiva frente a la ocurrencia de incidentes en los lugares de trabajo. La identificación de peligros se realiza mediante:

- Inspecciones (Formato de inspecciones planeadas Código 770,12,15-3)
- Investigación de accidentes de trabajo (Formato Informe de investigación Código: 770.12.15-15)

b. Identificación de peligros ("Matriz de identificación de peligros, valoración de riesgos y determinación de controles")

El Profesional especialista en SO, será el responsable de identificar los peligros presentes en los diferentes puestos de trabajo y actividades que se realizan. La identificación de peligros presentes en La Unidad para la Atención y Reparación Integral a las Victimas deberá considerar los siguientes aspectos:

- Identificar las actividades rutinarias y no rutinarias.
- Identificar los peligros asociados a las actividades desarrolladas por los funcionarios, contratistas y visitantes.
- Identificar comportamientos, capacidades y condiciones físicas de los funcionarios, contratistas y visitantes como posibles peligros.
- Identificar los peligros que se pueden generar fuera del sitio de trabajo que puedan afectar la salud y seguridad de los funcionarios, contratistas y visitantes.
- Peligros presentes alrededor de las instalaciones de la Unidad y de los lugares de trabajo (en caso de las Direcciones Territoriales).

- Condiciones de equipos, infraestructura y materiales proporcionados por La Unidad para la Atención y Reparación Integral a las Victimas presentes en los sitios de trabajo
- Identificar los peligros que se pueden generar en los cambios propuestos por la Unidad frente a sus actividades, procesos o materiales antes de ponerlos en marcha.
- Modificaciones que se puedan generar dentro del Sistema de Gestión SG SST
- El cumplimiento de requisitos legales aplicables a la Unidad.
- El diseño de puestos de trabajo, procesos, instalaciones, equipos, herramientas, actividades y el talento humano.

Para realizar dicha identificación se tendrá en cuenta la siguiente clasificación de acuerdo a la clasificación descrita en la Guía Técnica Colombiana GTC – 45, de posibles factores de riesgos que pueden afectar la salud y seguridad de los funcionarios, contratistas y visitantes de La Unidad para la Atención y Reparación Integral a las Víctimas.

Tabla de clasificación de factores de riesgo

Factores de Riesgo de Seguridad: Mecánicos, locativos, eléctricos.	• Incendio de sólidos, incendio de líquidos, incendio eléctrico, incendios combinados y explosiones. • Locativo, almacenamiento, trabajos de campo. • Caídas al mismo nivel • Caídas de objetos • Golpes o choques por objetos • Contacto directo • Contacto indirecto • Electricidad estática • Trabajo en alturas
Riesgo Biomecánico	• Posturas inadecuadas. • Movimientos repetitivos. • Manejo de cargas. • Carga postural estática • Diseño del puesto • Carga sensorial
Factores de Riesgo Biológico	• Virus • Bacterias • Hongos • Animales • Plantas
Factores de Riesgo Físico	• Ruido • Vibración

	• Iluminación deficiente o iluminación en exceso. • Radiación (Ionizante o no ionizante) • Disconfort térmico • Ventilación
Riesgo Psicosocial	• Relaciones Jerárquicas • Contenido de la Tarea • Nivel de Responsabilidad • Atención al Público. • Estrés individual • Estrés organizacional
Riesgo de Tránsito	• Colisión • Volcamiento • fallas en el vehículo (varada), obstáculos (condiciones de las vías). • atropellamiento.
Riesgo Público – Seguridad en las personas	• Factores Sociales • Factores Políticos • Seguridad Entorno
Riesgo Natural	• Terremotos • Inundaciones • Vendavales
Riesgo Químico	• Gases • Vapores • Humos • Neblinas
Humanos	• Actos inseguros, desacato de normas de seguridad. • Desconocimiento de prácticas preventivas, características físicas inadecuadas.

Esta información debe ser consignada en la "Matriz de identificación de peligros, valoración de riesgos y determinación de controles" teniendo en cuenta:

- **Factor de riesgo:** elemento que encierra una capacidad potencial de producir lesiones o daños materiales. Seleccione el factor de riesgo presente en el área o actividad en donde se están identificando las condiciones de trabajo teniendo en cuenta la tabla de clasificación de factores de riesgo.

- **Peligro:** Identifica el proceso, objetos, instrumentos y condiciones físicas y psicológicas de las personas que generan el factor de riesgo.

- **Actividad, proceso o tarea:** especifique la actividad, proceso o tarea en donde se están identificando las condiciones de trabajo.

- **Tipo de actividad:** puede ser rutinaria (Procedimientos normales) o No rutinarias (procedimientos periódicos y ocasionales)

- **Cargos:** mencione los cargos o niveles (administrativos, profesionales, directivos) directamente relacionados con los factores de riesgo identificados.

- **Origen:** marque con una X la fuente que identifico el factor de riesgo. Estas fuentes pueden ser (panorama, inspecciones, incidentes, programa PARE, observaciones del comportamiento y gestión del cambio)

c. Análisis del factor de riesgo

Se deberá determinar la descripción de las personas expuestas al factor de riesgo, posibles consecuencias, controles existentes y la valoración del riesgo para clasificar la tarea:

- **Expuestos:** número de personas que se ven afectadas en forma directa o indirecta por el factor de riesgo durante la realización del trabajo. Marque con una X si son visitantes, contratistas y/o trabajadores directos de La Unidad para la Atención y Reparación Integral a las Víctimas.

- **Efectos posibles a la salud:** describa brevemente las posibles consecuencias que pueden generar los peligros identificados sobre las personas expuestas.

- **Control existente:** medidas de eliminación o mitigación de los factores de riesgo que se han puesto en práctica en la fuente de origen, en el medio o en las personas.

- **Probabilidad:** es función de la frecuencia de exposición, la intensidad de la exposición, el número de expuestos y la sensibilidad especial de algunas de las personas al factor de riesgo, entre otras. Se clasifica en: **Baja** (el daño ocurrirá rara vez), **Media** (el daño ocurrirá en algunas ocasiones) y **Alta** (el daño ocurrirá siempre). Marque con una X según corresponda.

- **Consecuencia:** se estiman según el potencial de gravedad de las lesiones. Se clasifican en: Ligeramente **dañino** (lesiones superficiales, de poca gravedad, usualmente no incapacitantes o con incapacidades menores), **Dañino** (todas las EP no mortales, esguinces, torceduras, quemaduras de segundo o tercer grado, golpes severos, fracturas menores en costilla, dedo, mano no dominante, etc.) y **Extremadamente dañino** (lesiones graves: EP graves, progresivas y eventualmente mortales, fracturas de huesos grandes o de cráneo o múltiples, trauma encéfalocraneal, amputaciones, etc). Marque con una X según corresponda.

- **Estimación del riesgo:** está dada de acuerdo con la combinación realizada entre probabilidad y consecuencias, de la siguiente manera:

		CONSECUENCIAS		
		LIGERAMENTE DAÑINO	DAÑINO	EXTREMADAMENTE DAÑINO
PROBABILIDAD	BAJA	RIESGO TRIVIAL	RIESGO TOLERABLE	RIESGO MODERADO
	MEDIA	RIESGO TOLERABLE	RIESGO MODERADO	RIESGO IMPORTANTE
	ALTA	RIESGO MODERADO	RIESGO IMPORTANTE	RIESGO INTOLERABLE

- **Clasificación de la tarea:** determine si la actividad, proceso o tarea es CRITICA o NO CRITICA de acuerdo a los siguientes parámetros:

Estimación del riesgo (Trivial, Tolerable o Moderado) = Clasificación de la tarea NO CRITICA
Estimación del riesgo (Importante o Intolerable) = Clasificación de la tarea CRITICA.

d. Medidas de control

Una vez se determine la estimación del riesgo se debe identificar la intervención a seguir, para esto se deberá tener en cuenta la siguiente tabla:

RIESGO	RECOMENDACIONES
TRIVIAL	No se requiere acción específica si hay riesgos mayores.
TOLERABLE	No se necesita mejorar las medidas de control pero deben considerarse soluciones o mejoras de bajo costo y se deben hacer comprobaciones periódicas para asegurar que el riesgo aún es tolerable.
MODERADO	Se deben hacer esfuerzos por reducir el riesgo y en consecuencia debe diseñarse un proyecto de mitigación o control. Como está asociado a lesiones muy graves debe revisarse la probabilidad y

	debe ser de mayor prioridad que el moderado con menores consecuencias
IMPORTANTE	En presencia de un riesgo así no debe realizarse ningún trabajo. Este es un riesgo en el que se deben establecer estándares de seguridad o listas de verificación para asegurarse que el riesgo está bajo control antes de iniciar cualquier tarea. Si la tarea o la labor ya se han iniciado el control o reducción del riesgo debe hacerse cuanto antes.
INTOLERABLE	Si no es posible controlar este riesgo debe suspenderse cualquier operación o debe prohibirse su iniciación.

Las medidas de control a establecer para mitigar o eliminar el factor de riesgo identificado, tendrá en cuenta la siguiente jerarquización:

- **Eliminar:** consiste en prescindir de la actividad o equipo que genera el peligro. Esta medida de control contempla la eliminación de la tarea, actividad o equipo, con el fin de evitar la ocurrencia de algún incidente asociado.

- **Sustituir**: reemplazar la actividad o equipo por uno menos peligroso. Establece sustituir la actividad, tarea o equipo por otro, con el fin de evitar la ocurrencia de un incidente asociado o reducir la consecuencia del mismo.

- **Controles de ingeniería**: modificar las actividades o equipos de trabajo. Esta medida de control establece la remodelación de alguna actividad, tarea o equipo, con el fin de evitar la ocurrencia de un incidente asociado o reducir la consecuencia del mismo.

- **Señalización y/o gestiones administrativas**: aislar el peligro mediante barreras o su confinamiento. Se debe evitar que los incidentes potenciales de una actividad específica afecten la ejecución de otras actividades, por lo que se debe aislar la actividad, tarea o equipo. Esta medida de control también contempla gestiones administrativas como:

  - Realizar capacitación.
  - Elaborar Procedimientos de trabajo seguros específicos, planes, etc.
  - Elaboración de listas de chequeo, etc.
  - Realizar inspecciones de seguridad

- **En el trabajador, uso de EPP**: en donde el riesgo no es mayor o donde las anteriores medidas de control no se pueden implementar, se deberá desarrollar actividades que involucren al personal como capacitaciones, envió de información sobre el riesgo y dotación e inspección de elementos de protección personal.

- **Controles del comportamiento humano:** es el conjunto de actos exhibidos por el ser humano y determinados por la cultura, las actitudes, las emociones y los valores de la persona que se evidencian en las observaciones del comportamiento.

NOTA: las medidas de control que se determinen para eliminar o mitigar un riesgo debe considerar los posibles peligros que puede generar y el cumplimiento de los requisitos legales aplicables a la organización antes de su implementación.

e. Riesgo Residual

Una vez que los riesgos han sido valorizados se procede a evaluar la "calidad de la gestión", a fin de determinar cuán eficaces son los controles establecidos por la Unidad para mitigar los riesgos identificados. Finalmente, se calcula el "riesgo neto o residual".

El riesgo residual se calcula valorando la efectividad del control a implementar de acuerdo a la siguiente tabla:

EFECTIVIDAD DEL CONTROL

Control implementado	Efectividad
Ninguno	0,1
En el trabajador	0,5
Señalización, gestión administrativa y control de ingeniería	0,8
Eliminación y sustitución	1

Para hallar el riesgo residual (RR) aplicamos la siguiente fórmula:

RR = (Efectividad del control * Valoración del riesgo) – Valoración del riesgo

Una vez se determine el riesgo residual se realizara seguimiento a los riesgos que se encuentren valorados como "IMPORTANTES" e "INTOLERABLES" priorizando las actividades de mayor a menor valor estimado para el riesgo residual. Las medidas de control que se estimen en la "Matriz de identificación de peligros, valoración de riesgos y determinación de controles" se deberán incluir en los programas que desarrolle La Unidad para la Atención y Reparación Integral a las Víctimas, con el fin de realizar seguimiento a dichos controles.

f. Actualización de la matriz de identificación de peligros, valoración de riesgos y determinación de controles

La matriz de identificación de peligros, valoración de riesgos y determinación de controles para La Unidad para la Atención y Reparación Integral a las Víctimas deberá ser actualizada en los siguientes casos:

- Adquisición de máquinas y equipos
- Modificaciones en el acondicionamiento de los lugares de trabajo
- Cambio en las condiciones de trabajo

- La incorporación de un funcionario cuyas características personales o estado biológico conocido lo hagan especialmente sensible a las condiciones del puesto
- Incidentes ocurridos
- Rotación de personal
- Cambio en la normativa aplicable a las actividades de La Unidad para la Atención y Reparación Integral a las Víctimas en temas de seguridad y salud ocupacional.
- Hallazgos no considerados en las inspecciones y observaciones del comportamiento que se realicen
- Reportes de actos y condiciones inseguras no consideradas

NOTA: las modificadas realizadas a la matriz de identificación de peligros, valoración de riesgos y determinación de controles, así como las medidas de control determinadas para eliminar y/o mitigar la ocurrencia de incidentes deberán ser comunicadas a los funcionarios y contratistas por el Profesional Especialista en SO y/o Coordinadores.

ANEXO 3

Identificación riesgos de seguridad de la Información

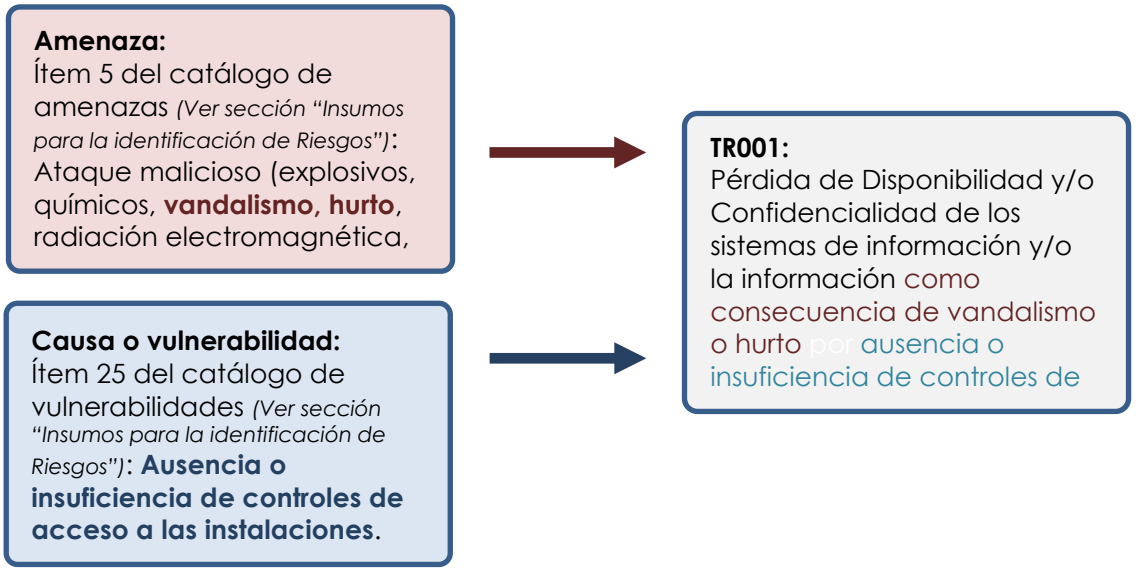
Para identificar los riesgos de seguridad de la información se debe tener realizar la identificación de las vulnerabilidades y amenazas que pueden afectar la Integridad, confidencialidad y disponibilidad de la información y los demás activos que la soportan.

Para la identificación es importante hacer claridad en los siguientes conceptos:

- Las amenazas todos los elementos o acciones capaces de atentar contra la seguridad de la información y son generadoras de eventos. Las amenazas surgen a partir de la existencia de vulnerabilidades, es decir que una amenaza sólo puede existir si existe una vulnerabilidad que pueda ser aprovechada.
- Las vulnerabilidades son las debilidades inherentes al activo que lo hacen susceptible de ser atacado.
- Los activos de información se refiere a la información que tiene valor para la organización y a los elementos relacionados con la misma o que la soportan, como por ejemplo sistemas, elementos de hardware, personas e instalaciones.

A modo de ejemplo, a continuación se selecciona el riesgo tipo TR001:

Pérdida de Disponibilidad y/o Confidencialidad de los sistemas de información y/o la información como consecuencia de vandalismo o hurto por ausencia o insuficiencia de controles de acceso a las áreas seguras.



a. Identificación de activos de información

Los riesgos de seguridad se identifican sobre activos previamente definidos, esta identificación se realiza de acuerdo al Procedimiento de Generación de Inventario de Activos de Información v1 el cual es responsabilidad del Proceso de gestión documental. Sin embargo como parte del proceso de identificación es importante relacionarlos en la descripción del riesgo. A continuación ejemplo para el diligenciamiento de la matriz de riesgos:

IDENTIFICACION					
No	**Proceso**	**Riesgo**	**Causas**	**Consecuencias**	**Tipo de Riesgo**
1		TR001*Pérdida de Disponibilidad y/o Confidencialidad de los sistemas de información y/o la información como consecuencia de vandalismo o hurto por ausencia o insuficiencia de controles de acceso a las áreas seguras. - Activo 1 (ID activo 1) - Activo 2 (ID activo 2)	Ausencia o insuficiencia de controles de acceso a las instalaciones.	Seguridad de la Información	Operativo
			Otros:		

b. Insumos para la identificación de Riesgos

Como parte de la identificación de riesgos la Unidad cuenta con algunas herramientas que facilitan esta labor, como son:

- Catálogo de amenazas
- Catálogo de causas o vulnerabilidades
- Tipos de riesgos establecidos

A continuación se observa el catálogo de amenazas que facilita la identificación de riesgos:

Catálogo de Amenazas	
No	**Fuentes o generadoras de eventos**
1	Uso de recursos (equipos de comunicación, medios de almacenamiento, sistemas de información, computadores) por personal no autorizado
2	Abuso de derechos por parte de usuario o administrador
3	Acceso a oficinas, edificio, sala, centro de cómputo, sistema de información, documentación, información, entre otros, por personal no autorizado

Catálogo de Amenazas	
No	**Fuentes o generadoras de eventos**
4	**Actos fraudulentos** (suplantación, fraude, venta de información, soborno, extorsión, falsificación de derechos, entre otros)
5	**Ataque malicioso** (explosivos, químicos, vandalismo, hurto, radiación electromagnética, entre otros).
6	Ataques contra el sistema (negación del servicio, manipulación de software, manipulación de equipo informático entre otros)
7	Cierre de operación de un proveedor o contratista crítico para la Entidad
8	**Código malicioso** (troyanos, gusanos, bomba lógica, entre otros)
9	Contaminación, Pandemias, virus
10	Daño físico (fuego, agua, humedad, contaminación química, construcción, entre otros)
11	Déficit de personal
12	Desastre natural (temblor, terremoto, inundación, incendio, rayos, contaminación química entre otros)
13	Destrucción de equipos o medios
14	Deterioro del sistema o medio de almacenaje
15	Divulgación de información por personal no autorizado
16	Funcionarios, contratistas o terceros (Acciones involuntarias y/o deliberadas)
17	Error en el uso (de equipos, medios, información, sistemas o servicios de información), por parte de usuarios
18	Errores de transmisión o almacenamiento
19	Espionaje (interceptación, ingeniería social**)**
20	Falla / degradación o mal funcionamiento del software o hardware
21	Falla de la red interna
22	**Falla de suministro de servicios esenciales** (agua, gas, aire acondicionado)
23	**Falla en el suministro de energía** (pérdida suministro de energía, planta eléctrica, UPS, banco de baterías)
24	Falla o corrupción del software.
25	Falla para respaldar la información.
26	**Falla sistema de comunicaciones** (Internet, canales, Radio, entre otros).
27	Fuego, agua, humedad, variaciones de temperatura/voltaje, radioactividad, polvo, gases, oxidación, campos electromagnéticos, entre otros.
28	Hurto o robo (información, documentos, medios o equipos)
29	Incumplimiento de leyes o regulaciones (propiedad intelectual, entre otros)
30	Incumplimiento de políticas o procedimientos internos.
31	Incumplimiento en el mantenimiento
32	Incumplimiento en el servicio de mantenimiento
33	Incumplimiento en los acuerdos de niveles de servicio
34	**Intrusión o acceso forzado** (instalaciones, sistemas de información, información)

Catálogo de Amenazas	
No	**Fuentes o generadoras de eventos**
35	**Intruso externo** (Ejemplo: Exempleados, delincuente informático, competidores)
36	**Pérdida de información** (contenida en documentación física o digital)
37	Piratería
38	Proveedor o contratista
39	Recuperación de medios reciclados o desechados
40	Saturación del sistema de información
41	Uso de software no licenciado o no autorizado

A continuación se encuentra el catálogo de causas o vulnerabilidades:

Catálogo de causas o vulnerabilidades	
No	**Ítem**
1	Acceso no controlado a información sensible / confidencial.
2	Acceso o uso no controlado del sistema de información (software, aplicativo).
3	Acceso o uso no controlado.
4	Almacenamiento de equipos sin protección.
5	Almacenamiento de información sin protección
6	Arquitectura insegura de la red.
7	Ausencia de "terminación/bloqueo de la sesión" cuando se abandona la estación de trabajo.
8	Ausencia de control de los activos que se encuentran fuera de las instalaciones.
9	Ausencia de controles y verificaciones en los procesos de selección y contratación de personal.
10	Ausencia de esquemas de respaldo.
11	Ausencia de registros de auditoría.
12	Ausencia de mecanismos de monitoreo a la actividad de los empleados y/o terceros.
13	Ausencia de planes de continuidad.
14	Ausencia de procedimiento de control de cambios.
15	Ausencia de procedimiento formal para la autorización de la información disponible al público.
16	Ausencia de responsables sobre la gestión en seguridad de la información y/o continuidad de negocio.
17	Ausencia de segmentación de la red.
18	Ausencia de sistemas y/o procedimientos de monitoreo de los recursos de procesamiento de información.
19	Ausencia o insuficiencia de procedimientos de control de cambios.
20	Ausencia o insuficiencia de actualizaciones.
21	Ausencia o insuficiencia de cláusulas contractuales y/o acuerdos de confidencialidad.

Catálogo de causas o vulnerabilidades	
No	**Ítem**
22	Ausencia o insuficiencia de contratos, acuerdos de nivel de servicio y/o confidencialidad con empleados o terceros.
23	Ausencia o insuficiencia de contratos, acuerdos de niveles de servicio y/o confidencialidad.
24	Ausencia o insuficiencia de control de cambios en la configuración.
25	Ausencia o insuficiencia de controles de acceso a las instalaciones.
26	Ausencia o insuficiencia de controles de monitoreo de las instalaciones (por ej. detección o extinción de incendios, líquidos inflamables, CCTV, entre otros).
27	Ausencia o insuficiencia de copias de respaldo.
28	Ausencia o insuficiencia de disposiciones (con respecto a la seguridad) en los contratos con los empleados y/o terceras partes.
29	Ausencia o insuficiencia de documentación de uso y/o administración.
30	Ausencia o insuficiencia de cláusulas contractuales y/o acuerdos de confidencialidad.
31	Hurto, fraude o sabotaje de equipos, medios, información o documentos.
32	Ausencia o insuficiencia de mantenimiento.
33	Ausencia o insuficiencia de mecanismos de identificación y autenticación.
34	Ausencia o insuficiencia de mecanismos de monitoreo de Red, gestión de la capacidad y disponibilidad.
35	Ausencia o insuficiencia de perfiles de acceso o falta de gestión de privilegios de acceso.
36	Ausencia o insuficiencia de planes de emergencia y simulacros de evacuación.
37	Ausencia o insuficiencia de políticas, procedimientos y directrices de seguridad.
38	Ausencia o insuficiencia de procedimientos de monitoreo de los recursos de procesamiento de información.
39	Ausencia o insuficiencia de procedimientos para el manejo información clasificada.
40	Ausencia o insuficiencia de procesos disciplinarios definidos en el caso de incidente de seguridad de la información.
41	Ausencia o insuficiencia de pruebas.
42	Ausencia o insuficiencia de un procedimiento para el manejo de comunicaciones externas.
43	Ausencia o insuficiencia de un proceso de análisis y tratamiento de riesgos.
44	Ausencia o insuficiencia de un proceso de gestión de incidentes de seguridad.
45	Ausencia o insuficiencia de un proceso para clasificar y etiquetar la información.
46	Ausencia o insuficiencia en el control de los activos que se encuentran fuera de las instalaciones.
47	Ausencia o insuficiencia en la definición y formalización de roles, funciones y responsabilidades en la seguridad de la información.
48	Ausencia o insuficiencia en la gestión de usuarios y contraseñas.
49	Canales de comunicación sin cifrado.
50	Capacidad inadecuada.

Catálogo de causas o vulnerabilidades	
No	**Ítem**
51	Conexión deficiente y/o desorganización del cableado estructurado / eléctrico.
52	Configuración incorrecta de parámetros o configuraciones por defecto.
53	Dependencia de personal clave, ausentismo y/o personal insuficiente.
54	Dependencia de proveedores.
55	Descarga y/o uso no controlado de software.
56	Desconocimiento, malinterpretación o no cumplimiento de las disposiciones legales, contractuales y/o regulatorias aplicables.
57	Disposición/reutilización de equipos sin borrado seguro.
58	Disposición/reutilización de medios de almacenamiento sin borrado seguro.
59	Documentación insuficiente o desactualizada.
60	Eliminación de información sin borrado seguro.
61	Especificaciones o requerimientos incompletos, inadecuados o no claros.
62	Falla en los servicios esenciales (internet, teléfonos, aire acondicionado, energía, agua, etc.).
63	Falla, daño o degradación de equipos.
64	Fallas conocidas o defectos del software.
65	Falta de protección contra virus y/o código malicioso
66	Falta de segregación de funciones o incorrecta aplicación de las mismas.
67	Incumplimiento de las condiciones técnicas y/o ambientales provistas por el fabricante.
68	Incumplimiento de políticas o procedimientos internos.
69	Insuficiente entrenamiento, capacitación o sensibilización.
70	Personal inconforme o molesto.
71	Proveedor o contratista único en el mercado.
72	Puertos o servicios activos no requeridos.
73	Punto único de falla.
74	Relojes no sincronizados.
75	Transferencia y/o almacenamiento de información en texto claro.
76	Testeo inadecuado o insuficiente
77	Ubicación geográfica de las instalaciones en una zona de alto impacto por eventos externos (desastres naturales, orden público, entre otros).
78	Uso de Software ilegal / No autorizado / Software Malicioso.

Teniendo en cuenta que riesgo es el potencial de que una amenaza pueda explotar una vulnerabilidad de un activo de información afectando la operación o imagen de la Entidad. Para facilitar la identificación de los riesgos de seguridad de la información, se establece un listado de riesgos comunes que asocian las amenazas y vulnerabilidades:

Listado de Riesgos comunes	
ID	**Riesgos**
TR001	Pérdida de Disponibilidad y/o Confidencialidad de los sistemas de información y/o la información como consecuencia de vandalismo o hurto por ausencia o insuficiencia de controles de acceso a las áreas seguras. - (A) Ataque malicioso (explosivos, químicos, vandalismo, hurto, radiación electromagnética, entre otros). - (V) Ausencia o insuficiencia de controles de acceso a las instalaciones.
TR002	Pérdida de Confidencialidad y/o Disponibilidad por hurto de equipos y/o Unidades de almacenamiento extraíbles en los que se almacene información sensible en texto claro, es decir no cifrado. - (A) Hurto o robo (información, medios o equipos) - (A) Incumplimiento de políticas o procedimientos internos. - (V) Ausencia o insuficiencia de procedimientos para el manejo información clasificada.
TR003	Pérdida de Confidencialidad y/o Integridad ocasionada por la infiltración en el sistema de información debido al acceso no autorizado como consecuencia de captura de credenciales transferidas en texto claro durante el ingreso vía web. - (A) Acceso no autorizado (a oficinas, edificio, sala, centro de cómputo, sistema de información, documentación, información, entre otros). - (A) Espionaje (interceptación, ingeniería social) - (V) Transferencia y/o almacenamiento de información en texto claro.
TR004	Pérdida de confidencialidad, integridad o disponibilidad ocasionada por la infiltración en el servidor y/o en el dispositivo de red debido al acceso no autorizado como consecuencia de captura de credenciales transferidas en texto claro. - (A) Acceso no autorizado (a oficinas, edificio, sala, centro de cómputo, sistema de información, documentación, información, entre otros). - (A) Espionaje (interceptación, ingeniería social) - (V) Transferencia y/o almacenamiento de información en texto claro.

Listado de Riesgos comunes	
ID	**Riesgos**
TR005	Pérdida de disponibilidad, integridad o confidencialidad de los sistemas de información y/o la información, debido a acciones involuntarias o deliberadas de empleados o terceros por la ausencia de mecanismos de monitoreo a la actividad de los usuarios. - (A) Empleados (Acciones involuntarias y/o deliberadas) - (A) Abuso de derechos (de usuario, administrador) - (A) Uso no autorizado de recursos (equipos de comunicación, medios de almacenamiento, sistemas de información, computadores) - (V) Ausencia de mecanismos de monitoreo a la actividad de los empleados y/o terceros. - (V) Ausencia de registros de auditoría.
TR006	Pérdida de confidencialidad de equipos de cómputo por hurto o daño fuera de las instalaciones debido a la ausencia o Insuficiencia de control de los activos. - (A) Hurto o robo (información, documentos, medios o equipos) - (V) Ausencia o insuficiencia en el control de los activos que se encuentran fuera de la instalaciones.
TR007	Pérdida de disponibilidad de información o acceso a sistemas críticos para la operación, debido a la insuficiencia de personal adecuado para cubrir funciones específicas. - (A) Déficit de personal - (V) Dependencia de personal clave, ausentismo y/o personal insuficiente. - (V) Documentación insuficiente o desactualizada. - (V) Ausencia o insuficiencia de documentación de uso y/o administración.

Listado de Riesgos comunes	
ID	**Riesgos**
TR008	Pérdida de disponibilidad de los equipos informáticos y/o de equipos de comunicaciones, debido a fallas en los equipos como resultado de la ausencia o insuficiencia de mantenimiento preventivo / correctivo a nivel físico. - (A) Falla, daño o degradación de equipos. - (A) Falla de suministro de servicios esenciales (agua, gas, aire acondicionado) - (A) Falla en el suministro de energía (pérdida suministro de energía, planta eléctrica, UPS, banco de baterías) - (V) Incumplimiento de las condiciones técnicas y/o ambientales provistas por el fabricante. - (V) Ausencia o insuficiencia de mantenimiento preventivo / correctivo. - (V) Arquitectura insegura de la red. - (A) Falla de la red interna. - (A) Falla de suministro de servicios esenciales (agua, gas, aire acondicionado) - (A) Falla / degradación o mal funcionamiento del software o hardware - (V) Fallas conocidas o defectos del software. - (V) Ausencia de segmentación de la red.
TR009	Pérdida de disponibilidad de los sistemas de información por ausencia o insuficiencia en la gestión de eventos de monitoreo. - (A) Falla / degradación o mal funcionamiento del software o hardware - (A) Empleados (Acciones involuntarias y/o deliberadas) - (A) Abuso de derechos (de usuario, administrador) - (V) Ausencia o insuficiencia de procedimientos de Monitoreo de los recursos de procesamiento de información.
TR010	Pérdida de Disponibilidad de los sistemas de información y/o información por insuficiencia o ausencia de planes de continuidad y/o contingencia ante un desastre y/o un evento mayor. - (A) Falla / degradación o mal funcionamiento del software o hardware. - (V) Ausencia de planes de continuidad y/o contingencia.
TR011	Pérdida de disponibilidad, confidencialidad y/o integridad del sistema de información por ataques internos o externos debidos a una arquitectura insegura de la red. - (A) Ataques contra el sistema (negación del servicio, manipulación de software, manipulación de equipo informático entre otros). - (V) Arquitectura insegura de la red. - (V) Puertos o servicios activos no requeridos.

Listado de Riesgos comunes	
ID	**Riesgos**
TR012	Pérdida de disponibilidad y/o integridad en el sistema al presentarse errores durante la ejecución de modificaciones debido a la falta de aplicación u omisión de alguna de las actividades del procedimiento de gestión de cambios. - (A) Empleados (Acciones involuntarias y/o deliberadas). - (A) Falla o corrupción del software. - (V) Ausencia o insuficiencia de un proceso de análisis y tratamiento de riesgos. - (V) Testeo inadecuado o insuficiente. - (V) Ausencia o insuficiencia de políticas, procedimientos y directrices de seguridad.
TR013	Pérdida de disponibilidad y/o integridad en la información en el sistema por errores en el uso o en la administración debido a documentación insuficiente o desactualizada o no seguir las directrices del fabricante. - (A) Error en el uso (de equipos, medios, información, sistemas o servicios de información). - (A) Empleados (Acciones involuntarias y/o deliberadas) - (V) Documentación insuficiente o desactualizada. - (V) Ausencia o insuficiencia de documentación de uso y/o administración. - (V) Ausencia o insuficiencia de políticas, procedimientos y directrices de seguridad.
TR014	Pérdida de disponibilidad, integridad y/o confidencialidad en el sistema de información debido a vulnerabilidades no corregidas explotadas por código malicioso. - (A) Código malicioso (troyanos, gusanos, bomba lógica, entre otros). - (V) Ausencia o insuficiencia de mantenimiento. - (V) Ausencia o insuficiencia de actualizaciones.
TR015	Pérdida de disponibilidad, integridad y/o confidencialidad en el sistema de información por la presencia de código malicioso debido a la falta de protección adecuada. - (A) Código malicioso (troyanos, gusanos, bomba lógica, entre otros). - (A) Ataques contra el sistema (negación del servicio, manipulación de software, manipulación de equipo informático entre otros). - (V) Falta de protección contra virus y/o código malicioso.
TR016	Pérdida de disponibilidad y/o integridad del sistema de información debido a ausencia o insuficiencia de copias de respaldo. - (A) Falla / degradación o mal funcionamiento del software o hardware. - (A) Falla o corrupción del software. - (A) Empleados (Acciones involuntarias y/o deliberadas) - (V) Ausencia o insuficiencia de copias de respaldo. - (V) Documentación insuficiente o desactualizada. - (V) Ausencia o insuficiencia de documentación de uso y/o administración.

Listado de Riesgos comunes	
ID	**Riesgos**
TR017	Pérdida de la confidencialidad en sistema de información debido a actividades de ingeniería social de un intruso que aproveche el desconocimiento de políticas, procedimientos y directrices de seguridad por parte de un colaborador, proveedor y/o terceras partes. - (A) Espionaje (interceptación, ingeniería social). - (A) Divulgación no autorizada. - (V) Ausencia o insuficiencia de políticas, procedimientos y directrices de seguridad. - (V) Insuficiente entrenamiento, capacitación o sensibilización. - (V) Ausencia de control de los activos que se encuentran fuera de la instalaciones. - (V) Acceso no controlado a información sensible / confidencial.
TR018	Pérdida parcial o total de disponibilidad de los sistemas de información y/o información como consecuencia de daño físico (Fuego, agua, humedad, variaciones de temperatura/voltaje, polvo, entre otros) por ausencia o insuficiencia de protección física contra desastres naturales. - (A) Daño físico (fuego, agua, humedad, contaminación química, construcción, entre otros) - (A) Desastre natural (temblor, terremoto, inundación, incendio, rayos, contaminación química entre otros) - (V) Ausencia o insuficiencia de controles de monitoreo de las instalaciones (por ej. detección o extinción de incendios, líquidos inflamables, CCTV, entre otros). - (A) Divulgación no autorizada - (V) Almacenamiento de información sin protección
TR019	Pérdida en la integridad de la Imagen y reputación de la entidad por incumplimiento de leyes y regulaciones ocasionadas por el uso de software no legal. - (A) Incumplimiento de leyes o regulaciones (propiedad intelectual, entre otros) - (A) Uso de software no licenciado o no autorizado - (A) Piratería - (V) Descarga y/o uso no controlado de software. - (V) Desconocimiento, malinterpretación o no cumplimiento de las disposiciones legales, contractuales y/o regulatorias aplicables. - (V) Uso de Software ilegal / No autorizado / Software Malicioso. - (V) Ausencia de responsables sobre la gestión en seguridad de la información y/o continuidad de negocio. - (V) Ausencia o insuficiencia de perfiles de acceso o falta de gestión de privilegios de acceso.

Listado de Riesgos comunes	
ID	**Riesgos**
TR020	Pérdida parcial o total de la disponibilidad de los sistemas de información y/o la información por ausencia o insuficiencia de Acuerdo de Nivel de Servicio como de confidencialidad con terceros. - (A) Proveedor o contratista - (A) Incumplimiento en los Acuerdo de nivel de servicio - (V) Ausencia o insuficiencia de contratos, acuerdos de niveles de servicio y/o confidencialidad. - (V) Ausencia o insuficiencia de disposiciones (con respecto a la seguridad) en los contratos con los empleados y/o terceras partes. - (V) Dependencia de proveedores. - (V) Falla de la red interna
TR021	Afectación de la Imagen y reputación de la entidad por incumplimiento normativo o de acuerdos de confidencialidad. - (A) Incumplimiento de leyes o regulaciones (propiedad intelectual, entre otros) - (A) Uso de software no licenciado o no autorizado - (A) Piratería - (V) Descarga y/o uso no controlado de software. - (V) Desconocimiento, malinterpretación o no cumplimiento de las disposiciones legales, contractuales y/o regulatorias aplicables. - (V) Uso de Software ilegal / No autorizado / Software Malicioso. - (V) Ausencia de responsables sobre la gestión en seguridad de la información y/o continuidad de negocio. - (V) Ausencia o insuficiencia de perfiles de acceso o falta de gestión de privilegios de acceso.
TR022	Interrupción total o parcial de la Disponibilidad debido a falla, daño o degradación de los sistemas (sistema contra incendio, CCTV, control de acceso, Sistema de Aire Acondicionado, Sistema de respaldo eléctrico, etc.) que garantiza la operación de los equipos en el Centro de Datos y centros de cableado, debido a falla eléctrica, degradación de equipos o falta de mantenimientos preventivos. - (A) Falla, daño o degradación de equipos. - (A) Falla de suministro de servicios esenciales (agua, gas, aire acondicionado) - (A) Falla en el suministro de energía (pérdida suministro de energía, planta eléctrica, UPS, banco de baterías) - (V) Incumplimiento de las condiciones técnicas y/o ambientales provistas por el fabricante. - (V) Ausencia o insuficiencia de mantenimiento preventivo / correctivo.

Listado de Riesgos comunes	
ID	**Riesgos**
TR023	Pérdida, robo, daño, alteración, divulgación no autorizada y/o fuga de información como consecuencia del acceso físico a las oficinas. -(A) Acceso no autorizado (a oficinas, edificio, sala, centro de cómputo, sistema de información, documentación, información, entre otros). -(A) Divulgación no autorizada -(V) Almacenamiento de equipos sin protección. -(V) Almacenamiento de información sin protección -(V) Hurto, fraude o sabotaje de equipos, medios, información o documentos.
TR024	Destrucción, pérdida, extravío, robo, daño o alteración de información en medio físico o lógico. -(A) Pérdida de información (contenida en documentación física o digital) -(A) Daño físico (fuego, agua, humedad, contaminación química, construcción, entre otros) -(V) Almacenamiento de equipos sin protección. -(V) Ausencia o insuficiencia de controles de acceso a las instalaciones. -(V) Ausencia o insuficiencia de controles de monitoreo de las instalaciones (por ej. detección o extinción de incendios, líquidos inflamables, CCTV, entre otros). -(A) Empleados (Acciones involuntarias y/o deliberadas). -(V) Ausencia de esquemas de respaldo. -(V) Acceso no controlado a información sensible / confidencial. -(A) Pérdida de información (contenida en documentación física o digital) -(A) Actos fraudulentos (suplantación, fraude, venta de información, soborno, extorsión, falsificación de derechos, entre otros) -(V) Acceso o uso no controlado del sistema de información (software, aplicativo). -(V) Ausencia o insuficiencia de políticas, procedimientos y directrices de seguridad. -(V) Dependencia de personal clave, ausentismo y/o personal insuficiente. -(V) Punto único de falla. -(V) Incumplimiento de políticas o procedimientos internos.
TR025	Pérdida de disponibilidad, integridad y/o confidencialidad en el sistema de información debido a accesos no autorizados. -(A) Acceso no autorizado (a oficinas, edificio, sala, centro de cómputo, sistema de información, documentación, información, entre otros). -(A) Divulgación no autorizada -(V) Acceso o uso no controlado del sistema de información (software, aplicativo). -(V) Ausencia de "terminación/bloqueo de la sesión" cuando se abandona la estación de trabajo. -(V) Insuficiente entrenamiento, capacitación o sensibilización. -(A) Pérdida de información (contenida en documentación física o digital). -(V) Ausencia o insuficiencia de procedimientos para el manejo información clasificada -(V) Error en el uso (de equipos, medios, información, sistemas o servicios de información)

Listado de Riesgos comunes	
ID	**Riesgos**
TR026	Pérdida, robo, daño, alteración, divulgación no autorizada y/o fuga de información como consecuencia de la interceptación no autorizada. -(A) Acceso no autorizado (a oficinas, edificio, sala, centro de cómputo, sistema de información, documentación, información, entre otros). -(A) Actos fraudulentos (suplantación, fraude, venta de información, soborno, extorsión, falsificación de derechos, entre otros) -(A) Empleados (Acciones involuntarias y/o deliberadas) -(A) Divulgación no autorizada -(A) Hurto o robo (información, documentos, medios o equipos) -(A) Pérdida de información (contenida en documentación física o digital) -(V) Acceso no controlado a información sensible / confidencial. -(V) Almacenamiento de información sin protección. -(V) Hurto, fraude o sabotaje de equipos, medios, información o documentos. -(V) Transferencia y/o almacenamiento de información en texto claro. -(A) Uso no autorizado de recursos (equipos de comunicación, medios de almacenamiento, sistemas de información, computadores) -(V) Ausencia o insuficiencia de un procedimiento para el manejo de comunicaciones externas.
TR027	Sanciones disciplinarias y/o penales a los funcionarios por la divulgación de información confidencial y por el incumplimiento de leyes y regulaciones, -(A) Actos fraudulentos (suplantación, fraude, venta de información, soborno, extorsión, falsificación de derechos, entre otros) -(A) Divulgación no autorizada -(A) Empleados (Acciones involuntarias y/o deliberadas). -(A) Incumplimiento de políticas o procedimientos internos. -(V) Ausencia de mecanismos de monitoreo a la actividad de los empleados y/o terceros. -(V) Ausencia o insuficiencia de contratos, acuerdos de nivel de servicio y/o confidencialidad con empleados o terceros. -(V) Personal inconforme o molesto.
TR028	Sanciones disciplinarias y/o penales a los funcionarios por la pérdida, daño, alteración y divulgación de las credenciales de gestión y administración de los equipos de cómputo y aplicativos. -(A) Acceso no autorizado (a oficinas, edificio, sala, centro de cómputo, sistema de información, documentación, información, entre otros). -(A) Empleados (Acciones involuntarias y/o deliberadas). -(A) Uso no autorizado de recursos (equipos de comunicación, medios de almacenamiento, sistemas de información, computadores) -(V) Ausencia o insuficiencia en la gestión de usuarios y contraseñas. -(V) Ausencia o insuficiencia de políticas, procedimientos y directrices de seguridad. -(V) Ausencia o insuficiencia de controles de acceso a las instalaciones. -(V) Acceso no controlado a información sensible / confidencial.

Listado de Riesgos comunes	
ID	**Riesgos**
TR029	Pérdida parcial o total de disponibilidad de los sistemas de información y/o información como consecuencia de atentado terrorista (Fuego, agua, humedad, variaciones de temperatura/voltaje, polvo, entre otros) por ausencia o insuficiencia de protección física contra desastres naturales. - (A) Ataque malicioso (explosivos, químicos, vandalismo, hurto, radiación electromagnética, entre otros). - (A) Destrucción de equipos o medios - (A) Pérdida de información (contenida en documentación física o digital) - (V) Ausencia o insuficiencia de controles de monitoreo de las instalaciones (por ej. detección o extinción de incendios, líquidos inflamables, CCTV, entre otros). - (V) Falla, daño o degradación de equipos. - (V) Ubicación geográfica de las instalaciones en una zona de alto impacto por eventos externos (desastres naturales, orden público, entre otros).
TR030	Pérdida de disponibilidad, integridad o confidencialidad de los sistemas de información y/o la información, debido a acciones involuntarias o deliberadas de empleados o terceros por la ausencia de mecanismos de monitoreo a la actividad de los usuarios. - (A) Empleados (Acciones involuntarias y/o deliberadas) - (A) Abuso de derechos (de usuario, administrador) - (A) Uso no autorizado de recursos (equipos de comunicación, medios de almacenamiento, sistemas de información, computadores) - (A) Saturación del sistema de información - (V) Ausencia de mecanismos de monitoreo a la actividad de los empleados y/o terceros. - (V) Ausencia de procedimiento de control de cambios. - (V) Ausencia de esquemas de respaldo. - (V) Hurto, fraude o sabotaje de equipos, medios, información o documentos. - (V) Ausencia de control de los activos que se encuentran fuera de la instalaciones. - (A) Pérdida de información (contenida en documentación física o digital) - (A) Intruso externo (Ejemplo: Exempleados, delincuente informático, competidores) - (V) Ausencia o insuficiencia de procedimientos para el manejo información clasificada.
TR031	Pérdida de disponibilidad, integridad y/o confidencialidad en el sistema de información debido a explotaciones de vulnerabilidades no corregidas. - (A) Ataques contra el sistema (negación del servicio, manipulación de software, manipulación de equipo informático entre otros) - (A) Código malicioso (troyanos, gusanos, bomba lógica, entre otros). - (V) Arquitectura insegura de la red. - (V) Ausencia o insuficiencia de mantenimiento. - (V) Ausencia o insuficiencia de actualizaciones. - (V) Ausencia o insuficiencia de procedimientos de monitoreo de los recursos de procesamiento de información.

Listado de Riesgos comunes	
ID	**Riesgos**
TR032	Interrupción Total o parcial de los procesos de negocio, por abuso de derechos, incumplimiento de los procesos y/o desconocimiento de las políticas de seguridad. -(A) Abuso de derechos (de usuario, administrador) -(A) Actos fraudulentos (suplantación, fraude, venta de información, soborno, extorsión, falsificación de derechos, entre otros) -(A) Empleados (Acciones involuntarias y/o deliberadas) -(A) Incumplimiento de políticas o procedimientos internos. -(V) Desconocimiento, malinterpretación o no cumplimiento de las disposiciones legales, contractuales y/o regulatorias aplicables. -(V) Ausencia o insuficiencia en la definición y formalización de roles, funciones y responsabilidades en la seguridad de la información.
TR033	Sanciones o procesos disciplinarios y/o penales y/o civiles por la divulgación no autorizada o fuga de información procesada y almacenada en medios físicos no autorizados. -(A) Uso no autorizado de recursos (equipos de comunicación, medios de almacenamiento, sistemas de información, computadores) -(A) Abuso de derechos (de usuario, administrador) -(A) Divulgación no autorizada -(V) Almacenamiento de información sin protección -(V) Ausencia o insuficiencia de contratos, acuerdos de nivel de servicio y/o confidencialidad con empleados o terceros. -(V) Transferencia y/o almacenamiento de información en texto claro.
TR034	Sanciones, demandas y/o pérdidas económicas como consecuencia por la pérdida, daño, alteración, divulgación no autorizada o fuga de la información registrada en medio físico o electrónico. -(A) Acceso no autorizado (a oficinas, edificio, sala, centro de cómputo, sistema de información, documentación, información, entre otros). -(A) Hurto o robo (información, documentos, medios o equipos) -(V) Ausencia o insuficiencia de controles de acceso a las instalaciones. -(V) Hurto, fraude o sabotaje de equipos, medios, información o documentos. -(V) Ausencia o insuficiencia en el control de los activos que se encuentran fuera de la instalaciones.
TR035	Pérdida de Confidencialidad y/o Disponibilidad de la información por acceso no autorizado a la información almacenada en equipos de cómputo, medio digital y/o físico - (A) Hurto o robo (información, medios o equipos) - (A) Incumplimiento de políticas o procedimientos internos. - (V) Ausencia o insuficiencia de procedimientos para el manejo información clasificada.

Listado de Riesgos comunes	
ID	**Riesgos**
TR036	Acciones disciplinarias y/o penales y/o civiles por desacato, como consecuencia del incumplimiento de los términos por la pérdida o daño de la documentación -(A) Error en el uso (de equipos, medios, información, sistemas o servicios de información) -(A) Falla para respaldar la información. -(V) Ausencia de esquemas de respaldo. -(V) Ausencia o insuficiencia de procedimientos para el manejo información clasificada. -(A) Hurto o robo (información, documentos, medios o equipos) -(V) Ausencia o insuficiencia en el control de los activos que se encuentran fuera de la instalaciones. -(A) Falla sistema de comunicaciones (Internet, canales, Radio, entre otros). -(V) Ausencia de planes de continuidad. -(A) Acceso o uso no controlado.
TR037	Incumplimiento legal, regulatorio y/o normativo por la pérdida, daño, alteración, divulgación no autorizada o fuga de información debido a insuficiencias en los mecanismos establecidos para la gestión de los documentos públicos, físicos y electrónicos en cuanto a procesos tales como la producción o recepción, la distribución, la consulta, la organización, la recuperación y la disposición final de los documentos. -(A) Acceso no autorizado (a oficinas, edificio, sala, centro de cómputo, sistema de información, documentación, información, entre otros). -(A) Divulgación no autorizada -(A) Pérdida de información (contenida en documentación física o digital) -(V) Ausencia o insuficiencia de controles de acceso a las instalaciones. -(V) Ausencia o insuficiencia de disposiciones (con respecto a la seguridad) en los contratos con los empleados y/o terceras partes. -(V) Desconocimiento, malinterpretación o no cumplimiento de las disposiciones legales, contractuales y/o regulatorias aplicables. -(V) Acceso no controlado a información sensible / confidencial.
TR038	Pérdida de Confidencialidad, Integridad y/o disponibilidad de la información, ocasionada por la alteración, destrucción o robo de los medios físico de almacenamiento. -(A) Destrucción de equipos o medios -(A) Empleados (Acciones involuntarias y/o deliberadas) -(V) Acceso no controlado a información sensible / confidencial. -(V) Personal inconforme o molesto. -(V) Falla, daño o degradación de equipos. -(A) Pérdida de información (contenida en documentación física o digital) -(V) Ausencia o insuficiencia de políticas, procedimientos y directrices de seguridad. -(A) Errores de transmisión o almacenamiento

Listado de Riesgos comunes	
ID	**Riesgos**
TR039	Pérdida de la confidencialidad, integridad y disponibilidad de la información por hurto de los medios de almacenamiento físico. -(A) Uso no autorizado de recursos (equipos de comunicación, medios de almacenamiento, sistemas de información, computadores) -(A) Destrucción de equipos o medios -(A) Hurto o robo (información, documentos, medios o equipos) -(V) Almacenamiento de información sin protección -(V) Ausencia de mecanismos de monitoreo a la actividad de los empleados y/o terceros. -(V) Hurto, fraude o sabotaje de equipos, medios, información o documentos.
TR040	Afectación de la Imagen y reputación de la entidad por incumplimiento normativo o de acuerdos de confidencialidad. - (A) Incumplimiento de leyes o regulaciones (propiedad intelectual, entre otros) - (A) Piratería - (V) Desconocimiento, malinterpretación o no cumplimiento de las disposiciones legales, contractuales y/o regulatorias aplicables. - (V) Ausencia de responsables sobre la gestión en seguridad de la información.
TR041	Pérdida de la confidencialidad, integridad y disponibilidad de la información por acceso y uso no autorizado de la información. -(A) Divulgación no autorizada -(A) Error en el uso (de equipos, medios, información, sistemas o servicios de información) -(A) Pérdida de información (contenida en documentación física o digital) -(v) Ausencia de procedimiento formal para la autorización de la información disponible al público. -(v) Ausencia o insuficiencia de perfiles de acceso o falta de gestión de privilegios de acceso. -(v) Ausencia o insuficiencia en la gestión de usuarios y contraseñas. -(v) Disposición/reutilización de equipos sin borrado seguro.
TR042	Pérdida de Disponibilidad y/o Confidencialidad de la información registrada en documento físico, como consecuencia de vandalismo o hurto por ausencia de mecanismos de control. - (A) Hurto o robo (información, documentos, medios o equipos) - (V) Ausencia o insuficiencia de controles de acceso a las instalaciones.

Listado de Riesgos comunes	
ID	**Riesgos**
TR043	Pérdida de Confidencialidad, integridad y/o Disponibilidad de la información por acceso no autorizado a la información almacenada en medio digital y/o físico. -(A) Acceso no autorizado (a oficinas, edificio, sala, centro de cómputo, sistema de información, documentación, información, entre otros). -(A) Actos fraudulentos (suplantación, fraude, venta de información, soborno, extorsión, falsificación de derechos, entre otros) -(A) Empleados (Acciones involuntarias y/o deliberadas) -(A) Divulgación no autorizada -(A) Hurto o robo (información, documentos, medios o equipos) -(A) Pérdida de información (contenida en documentación física o digital) -(V) Acceso no controlado a información sensible / confidencial. -(V) Almacenamiento de información sin protección. -(V) Hurto, fraude o sabotaje de equipos, medios, información o documentos. -(V) Transferencia y/o almacenamiento de información en texto claro.
TR044	Pérdida de Integridad y/o confidencialidad de la información por acceso no autorizado a los sistemas de información (A) Acceso no autorizado (a oficinas, edificio, sala, centro de cómputo, sistema de información, documentación, información, entre otros). (A) Empleados (Acciones involuntarias y/o deliberadas) (A) Hurto o robo (información, documentos, medios o equipos) (V) Acceso o uso no controlado del sistema de información (software, aplicativo). (V) Ausencia o insuficiencia de contratos, acuerdos de nivel de servicio y/o confidencialidad con empleados o terceros. (V) Ausencia o insuficiencia de perfiles de acceso o falta de gestión de privilegios de acceso. (V) Ausencia o insuficiencia en la definición y formalización de roles, funciones y responsabilidades en la seguridad de la información. (A) Actos fraudulentos (suplantación, fraude, venta de información, soborno, extorsión, falsificación de derechos, entre otros) (V) Ausencia de "terminación/bloqueo de la sesión" cuando se abandona la estación de trabajo.

Listado de Riesgos comunes	
ID	**Riesgos**
TR045	Pérdida de confidencialidad e integridad de la información por acceso no autorizado a los sistemas de información. (A) Uso no autorizado de recursos (equipos de comunicación, medios de almacenamiento, sistemas de información, computadores) (A) Actos fraudulentos (suplantación, fraude, venta de información, soborno, extorsión, falsificación de derechos, entre otros) (A) Falla / degradación o mal funcionamiento del software o hardware (A) Pérdida de información (contenida en documentación física o digital) (V) Acceso o uso no controlado del sistema de información (software, aplicativo). (V) Ausencia de esquemas de respaldo. (V) Ausencia o insuficiencia de cláusulas contractuales y/o acuerdos de confidencialidad. (V) Transferencia y/o almacenamiento de información en texto claro.
TR046	Pérdida de Confidencialidad y/o Disponibilidad de la información almacenada en medio físico, por el incumplimiento de políticas de seguridad de la información. - (A) Hurto o robo (información, medios o equipos) - (A) Incumplimiento de políticas o procedimientos internos. - (V) Ausencia o insuficiencia de procedimientos para el manejo información clasificada. - (V) Eliminación de información sin borrado seguro.
TR047	Pérdida de Disponibilidad de los sistemas de información y/o información por daños o degradación de los sistemas de información. - (A) Deterioro del sistema o medio de almacenaje - (A) Falla / degradación o mal funcionamiento del software o hardware. - (V) Fallas conocidas o defectos del software. - (A) Error en el uso (de equipos, medios, información, sistemas o servicios de información). - (A) Falla sistema de comunicaciones (Internet, canales, Radio, entre otros). - (V) Falla en los servicios esenciales (internet, teléfonos, aire acondicionado, energía, agua, etc.). - (V) Ausencia de planes de continuidad. - (A) Falla o corrupción del software. - (V) Ausencia o insuficiencia de control de cambios en la configuración.

Listado de Riesgos comunes	
ID	**Riesgos**
TR048	Sanciones disciplinarias y/o penales a los funcionarios por la pérdida, daño, alteración y divulgación de información confidencial y por el incumplimiento de las leyes y regulaciones. -(A) Actos fraudulentos (suplantación, fraude, venta de información, soborno, extorsión, falsificación de derechos, entre otros) -(A) Empleados (Acciones involuntarias y/o deliberadas). -(A) Divulgación no autorizada -(A) Incumplimiento de políticas o procedimientos internos. -(V) Ausencia o insuficiencia de políticas, procedimientos y directrices de seguridad. -(V) Personal inconforme o molesto. -(V) Desconocimiento, malinterpretación o no cumplimiento de las disposiciones legales, contractuales y/o regulatorias aplicables. -(V) Almacenamiento de equipos sin protección.
TR049	Destrucción, pérdida, extravío, robo, daño o alteración de información en medio físico o lógico. -(A) Daño físico (fuego, agua, humedad, contaminación química, construcción, entre otros) -(A) Destrucción de equipos o medios -(A) Deterioro del sistema o medio de almacenaje -(A) Pérdida de información (contenida en documentación física o digital) -(V) Ausencia de mecanismos de monitoreo a la actividad de los empleados y/o terceros. -(V) Falla, daño o degradación de equipos. -(V) Insuficiente entrenamiento, capacitación o sensibilización. -(A) Errores de transmisión o almacenamiento -(V) Punto único de falla. -(V) Almacenamiento de información sin protección
TR050	Destrucción, pérdida, extravío, robo, daño o alteración de información en medio físico. -(A) Daño físico (fuego, agua, humedad, contaminación química, construcción, entre otros) -(A) Hurto o robo (información, documentos, medios o equipos) -(A) Pérdida de información (contenida en documentación física o digital) -(V) Hurto, fraude o sabotaje de equipos, medios, información o documentos. -(V) Ausencia o insuficiencia de procedimientos para el manejo información clasificada.
TR051	Pérdida de Confidencialidad, Integridad y/o disponibilidad de la información, ocasionada por el acceso no autorizado a la información, almacenada en los diferentes sistemas de información y/o Unidades de almacenamiento. -(A) Acceso no autorizado (a oficinas, edificio, sala, centro de cómputo, sistema de información, documentación, información, entre otros). -(A) Error en el uso (de equipos, medios, información, sistemas o servicios de información) -(A) Hurto o robo (información, documentos, medios o equipos) -(V) Almacenamiento de información sin protección -(V) Hurto, fraude o sabotaje de equipos, medios, información o documentos. -(V) Ausencia o insuficiencia de perfiles de acceso o falta de gestión de privilegios de acceso.

Listado de Riesgos comunes	
ID	**Riesgos**
TR052	Interrupción parcial o total, de los servicios tecnológicos suministrados por el centro de datos, debido a fallas en la administración y gestión de los dispositivos de Red. -(A) Ataques contra el sistema (negación del servicio, manipulación de software, manipulación de equipo informático entre otros) -(v) Arquitectura insegura de la red. -(V) Ausencia o insuficiencia de mecanismos de monitoreo de Red, gestión de la capacidad y disponibilidad. -(A) Falla de la red interna. -(v) Ausencia o insuficiencia de un proceso de gestión de incidentes de seguridad. -(v) Falla, daño o degradación de equipos.
TR053	Sanciones y/o demandas por el incumplimiento de las regulaciones y los acuerdos de Nivel de Servicio. -(A) Incumplimiento de leyes o regulaciones (propiedad intelectual, entre otros) -(A) Incumplimiento en los Acuerdo de Nivel de Servicio. -(V) Desconocimiento, malinterpretación o no cumplimiento de las disposiciones legales, contractuales y/o regulatorias aplicables. -(V) Falta de segregación de funciones o incorrecta aplicación de las mismas.
TR054	Pérdida, robo, daño, alteración, divulgación no autorizada y/o fuga de información como consecuencia del acceso físico al Data center. -(A) Acceso no autorizado (a oficinas, edificio, sala, centro de cómputo, sistema de información, documentación, información, entre otros). -(A) Divulgación no autorizada -(V) Almacenamiento de información sin protección -(V) Incumplimiento de políticas o procedimientos internos.

Control de cambios

Versión	Ítem del cambio	Cambio realizado	Motivo del cambio	Fecha del cambio
V1	Creación	NA	NA	NA
V2	Metodología	Actualización por cambios en el MECI 1000:2005 y queda vigente el MECI 2014.	Actualización	

		Expedición del Decreto 0943 de 2014		
V2	Metodología	Ajustes por la expedición de la Guía para la Administración del Riesgo del DAFP	Actualización	
V3	Metodología	Ajustes por la Actualización de la Guía para la Administración del Riesgo del DAFP	Actualización	27/04/2016
V3	Metodología	Ajustes por la expedición de la Guía para la gestión del riesgo de corrupción	Actualización	27/04/2016
V4	Metodología	Inclusión y articulación de riesgos públicos, ambientales, seguridad y salud en el trabajo y seguridad de la información	Actualización	03/03/2017