MANUAL DE ADMINISTRACIÓN DEL RIESGO
SANATORIO DE CONTRATACIÓN ESE

CONTENIDO

INTRODUCCIÓN

La administración de riesgos es reconocida como una parte integral de las buenas prácticas gerenciales, tanto pública como privada, la cual cobra mayor importancia dado el dinamismo y los constantes cambios que el mundo globalizado de hoy exige. Estos cambios hacen que las entidades se enfrenten a factores internos y/o externos que pueden crear incertidumbre sobre el logro de los objetivos planteados.

El Sanatorio de Contratación E.S.E., comprometido con la calidad en la prestación del servicio de salud integral a los enfermos de Hansen y sus convivientes, así como a la población sana del Municipio de Contratación y su área de influencia, implementará una Política de Administración del Riesgo que permita controlar aquellos que puedan impedir el logro de los objetivos institucionales y de procesos, identificándolos, evaluándolos y estableciendo las acciones a llevar a cabo para su prevención, contando para ello con personal comprometido con el mejoramiento continuo de sus procesos, quienes evaluarán la efectividad de las acciones y controles establecidos.

La Política de Administración del Riesgo del Sanatorio de Contratación E.S.E., se basó en la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas. Versión 2 expedida por el Departamento Administrativo de la Función Pública (DAFP) en 2022, la cual tiene como fin unificar los lineamientos en los aspectos comunes de las metodologías para la administración de los riesgos y fortalecer el enfoque preventivo con el fin de facilitar a las entidades, la identificación y tratamiento de cada uno de ellos.

1. OBJETIVOS

1.1. OBJETIVO GENERAL

Establecer los elementos y marco general para el control y la gestión del riesgo del Sanatorio de Contratación E.S.E, que permita a los funcionarios identificar, analizar, valorar y controlar los riesgos, que crean incertidumbre en el logro de los objetivos propuestos en cada proceso, definiendo las alternativas de acción encaminadas a reducirlos y/o mitigarlos, dando un adecuado tratamiento, a fin de garantizar el cumplimiento de la misión, visión y los objetivos institucionales.

1.2. OBJETIVOS ESPECÍFICOS

- Generar una visión sistémica acerca de la administración y evaluación de los riesgos.
- Aumentar la probabilidad de alcanzar los objetivos y proporcionar un aseguramiento razonable con respecto al logro de estos.
- Proteger los recursos del Sanatorio de Contratación E.S.E., resguardándolos contra la materialización de los riesgos.
- Concientizar la necesidad de identificar y tratar los riesgos en todos los niveles de la entidad.
- Involucrar y comprometer a todos los servidores del Sanatorio de Contratación E.S.E., en la búsqueda de acciones encaminadas a prevenir y administrar los riesgos.
- Mejorar la eficacia y eficiencia operativa de la institución.
- Asegurar el cumplimiento normas, leyes y regulaciones.
- Identificar situaciones que, por sus características, pueden originar prácticas corruptas.

2. ALCANCE

La Política de Administración del Riesgo del Sanatorio de Contratación E.S.E., aplica para todas los procesos y dependencias de la entidad y deben ser conocidas, aplicadas y cumplidas tanto por los servidores públicos como por los contratistas que apoyan la gestión y demás partes implicadas.

3. MARCO LEGAL

El riesgo y su administración están fundamentados en el siguiente marco normativo:

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, artículo 2 literal a). Proteger los recursos de la organización, buscando su adecuada administración ante posibles riesgos que los afectan y 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.

Ley 610 de 2000, por la cual se establece el trámite de los procesos de responsabilidad fiscal de competencia de las contralorías.

Ley 1474 de 2011, Estatuto Anticorrupción. Artículo 73. “Plan Anticorrupción y de Atención al Ciudadano” que deben elaborar anualmente todas las entidades, incluyendo el mapa de riesgos de corrupción, las medidas concretas para mitigar estos riesgos, las estrategias Antitrámites y los mecanismos para mejorar la atención al ciudadano. Decreto 2641 del 17 de diciembre del 2012, por el cual se reglamenta los artículos 73 y 76 de la ley 1474 de 2011.

Decreto 2641 de 2012, “Por el cual se reglamentan los artículos 73 y 76 de la Ley 1474 de 2011”: ARTÍCULO 1. Señálese como metodología para diseñar y hacer seguimiento a la estrategia de lucha contra la corrupción y de atención al ciudadano de que trata el artículo 73 de la Ley 1474 de 2011, la establecida en el Plan Anticorrupción y de Atención al Ciudadano contenida en el documento “Estrategias para la Construcción del Plan Anticorrupción y de Atención al Ciudadano”.

Ley 1581 de 2012, Por la cual se dictan disposiciones generales para la protección de datos personales.

Ley 1712 de 2014, Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.

Decreto 1083 de 2015, "Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública": CAPÍTULO 5 "Elementos técnicos y administrativos que fortalezcan el Sistema de Control Interno en las entidades y organismos del Estado", ARTÍCULO 2.2.21.5.4 "Administración de riesgos". Como parte integral del fortalecimiento de los sistemas de control interno en las entidades públicas las autoridades correspondientes establecerán y aplicarán políticas de administración del riesgo. Para tal efecto, la identificación y análisis del riesgo debe ser un proceso permanente e interactivo entre la administración y las oficinas de control interno o quien haga sus veces, evaluando los aspectos tanto internos como externos que pueden llegar a representar amenaza para la consecución de los objetivos organizaciones, con miras a establecer acciones efectivas, representadas en actividades de control, acordadas entre los responsables de las áreas o procesos y las oficinas de control interno e integradas de manera inherente a los procedimientos.

Decreto 648 de 2017, "Por el cual se modifica y adiciona el Decreto 1083 de 2015, Reglamentario Único del Sector de la Función Pública": SECCIÓN 2 "Protección Especial" ARTÍCULO 2.2.21.1.6 "Funciones del Comité Institucional de Coordinación de Control Interno". Literal g. Someter a aprobación del representante legal la política de administración del riesgo y hacer seguimiento, en especial a la prevención y detección de fraude y mala conducta.

Decreto 1499 de 2017, "Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015": TÍTULO 23 Articulación del Sistema de Gestión con los Sistemas de Control Interno. ARTÍCULO 2.2.23.2. "Actualización del Modelo Estándar de Control Interno". La actualización del Modelo Estándar de Control Interno para el Estado Colombiano – MECI, se efectuará a través del Manual Operativo del Modelo Integrado de Planeación y Gestión – MIPG, el cual será de obligatorio cumplimiento y aplicación para las entidades y organismos a que hace referencia el artículo 5 de la Ley 87 de 1993.

Decreto 403 de 2020, Por el cual se dictan normas para la correcta implementación del Acto Legislativo 04 de 2019 y el fortalecimiento del control fiscal.

Ley 2195 de 2022, Por medio de la cual se adoptan medidas en materia de transparencia, prevención y lucha contra la corrupción y se dictan otras disposiciones.

4. TÉRMINOS Y DEFINICIONES[1]

- **Activo:** En el contexto de seguridad digital son elementos tales como aplicaciones de la organización, servicios web, redes, Hardware, información física o digital, recurso humano, entre otros, que utiliza la organización para funcionar en el entorno digital.

- Bien público: Son todos aquellos muebles e inmuebles de propiedad pública (este concepto comprende: bienes del Estado y aquellos productos del ejercicio de una función pública a cargo de particulares). Estos se clasifican en bienes de uso público y bienes fiscales, definidos así:

  a. Bien de uso público: aquellos cuyo uso pertenece a todos los habitantes del territorio nacional. Ejemplos: Las calles, plazas, puentes, vías, parques etc.
  b. Bienes fiscales: aquellos que están destinados al cumplimiento de las funciones públicas o servicios públicos (Consejo de Estado, 2012), es decir, afectos al desarrollo de su misión y utilizados para sus actividades. Ejemplos: Los terrenos, edificios, oficinas, colegios, hospitales, otras construcciones, fincas, granjas, equipos, enseres, mobiliario etc.

- **Apetito de riesgo:** Es el nivel de riesgo que la entidad puede aceptar, relacionado con sus Objetivos, el marco legal y las disposiciones de la Alta Dirección y del Órgano de Gobierno. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.

- **Capacidad de riesgo:** Es el máximo valor del nivel de riesgo que una Entidad puede soportar y a partir del cual se considera por la Alta Dirección y el Órgano de Gobierno que no sería posible el logro de los objetivos de la Entidad.

- **Causa:** todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo

- **Causa Inmediata:** Circunstancias bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo.

- **Causa Raíz:** Causa principal o básica, corresponde a las razones por la cuales se puede presentar el riesgo. Factores de Riesgo: Son las fuentes generadoras de riesgos.

- **Confidencialidad:** Propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados

[1] Guía para la Administración del Riesgo y el diseño de controles en entidades públicas Versión 6. Función Pública. Dirección de Gestión y Desempeño Institucional noviembre 2022

- **Consecuencia**: los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas.

- **Gestión del Riesgo Fiscal:** son las actividades que debe desarrollar cada Entidad y todos los gestores públicos (ver concepto de gestor público) para identificar, valorar, prevenir y mitigar los riesgos fiscales (probabilidad de efecto dañoso sobre los bienes, recursos y/o intereses patrimoniales de naturaleza pública, a causa de un evento potencial).

- **Gestor público:** Es todo aquel que participa, concurre, incide o contribuye directa o indirectamente en el manejo o administración de bienes, recursos o intereses patrimoniales de naturaleza pública, sean o no gestores fiscales, por lo tanto, son todos los gestores públicos y no sólo los que desarrollan gestión fiscal, los llamados a prevenir riesgos fiscales". A título de ejemplo, además de los gestores fiscales, son gestores públicos, entre otros (sin perjuicio de las particularidades de cada entidad): los contratistas, los interventores, los supervisores y en general todos los servidores públicos.

- **Gestor Fiscal:** Son los servidores públicos y las personas de derecho privado que manejen o administren recursos o fondos públicos, desarrollando actividades económicas, jurídicas y tecnológicas, tendientes a la adecuada y correcta adquisición, planeación, conservación, administración, custodia, explotación, enajenación, consumo, adjudicación, gasto, inversión y disposición de los bienes públicos, así como, a la recaudación, manejo e inversión de sus rentas, en orden a cumplir los fines esenciales del Estado (artículo 3 de la Ley 610 de 2000 o la norma que lo sustituya o modifique)" . A título de ejemplo son gestores fiscales, entre otros (sin perjuicio de las particularidades de cada entidad): representante legal, ordenador del gasto, autorizado para contratar, pagador, tesorero, almacenista.

- **Impacto:** las consecuencias que puede ocasionar a la organización la materialización del riesgo.

- **Integridad:** Propiedad de exactitud y completitud. Disponibilidad: Propiedad de ser accesible y utilizable a demanda por una entidad.

- **Intereses patrimoniales de naturaleza pública:** Son expectativas razonables de beneficios, que en condiciones normales se espera obtener o recibir y que sean susceptible de estimación económica. A diferencia del recurso público, los intereses patrimoniales de naturaleza pública son expectativas. Ejemplos: Son algunos ejemplos de intereses patrimoniales de naturaleza pública, la rentabilidad proyectada de cualquier inversión pública, es decir antes de que se causen o generen efectivamente; la cobertura de garantías y pólizas; la participación accionaria pública en una empresa de economía mixta o en una empresa de servicios públicos con socio o socios públicos; los rendimientos financieros y frutos de recursos públicos cuando se proyectan, es decir

antes de que se causen o generen efectivamente; así como, los intereses moratorios, indexaciones, actualización del dinero en el tiempo, estimación de pérdida de costo de oportunidad, cuando se trata de cobrar recursos públicos que un tercero debe; explotación de bienes públicos y/o recaudo de recursos públicos por un particular sin contrato o habilitación legal.

- **Nivel de riesgo:** Es el valor que se determina a partir de combinar la probabilidad de ocurrencia de un evento potencialmente dañino y la magnitud del impacto que este evento traería sobre la capacidad institucional de alcanzar los objetivos. En general la fórmula del Nivel del Riesgo poder ser Probabilidad * Impacto, sin embargo, pueden relacionarse las variables a través de otras maneras diferentes a la multiplicación, por ejemplo, mediante una matriz de Probabilidad – Impacto.

- **Patrimonio público:** se entiende como el conjunto de bienes o recursos o intereses patrimoniales de naturaleza pública, susceptibles de estimación económica (artículo 6 Ley 610 de 2000 y sentencia C340-07).

- **Recurso público:** Para efectos del capítulo de riesgos fiscales, entiéndase como recurso público, los dineros comprometidos y ejecutados en ejercicio de la función pública. Ejemplos: Los recursos de inversión y recursos de funcionamiento de cada entidad; los recursos generados por actividades comerciales, industriales y de prestación de servicios, por parte de entidades estatales; los recursos parafiscales; los recursos que resultan del ejercicio de funciones públicas por particulares.

- **Riesgo:** Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales.

  Nota: Los eventos potenciales hacen referencia a la posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos.

- **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 fiscal:** Es el efecto dañoso sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública, a causa de un evento potencial (ver conceptos de recursos públicos, bien público e Intereses patrimoniales de naturaleza pública).

- **Riesgo Inherente:** Nivel de riesgo propio de la actividad. El resultado de combinar la probabilidad con el impacto nos permite determinar el nivel del riesgo inherente, dentro de unas escalas de severidad.

- **Riesgo Residual:** El resultado de aplicar la efectividad de los controles al riesgo inherente. Control: Medida que permite reducir o mitigar un riesgo.

- **Tolerancia del riesgo:** Es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del Apetito de riesgo determinado por la entidad.

- **Vulnerabilidad:** Representan la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.

5. ESTABLECIMIENTO DEL CONTEXTO ESTRATÉGICO Y POR PROCESOS

El contexto estratégico permite de manera apropiada la identificación de los riesgos, dado que se precisan los objetivos institucionales y los objetivos de los procesos, y como se lograrán.

Por lo tanto, partiendo de la dimensión del Direccionamiento Estratégico y la Planeación en el cual se evalúan y determinan los factores internos y externos que interactúan con la gestión y la ruta a seguir para lograr los objetivos, también provee información relevante y otorga la articulación debida a la Administración de Riesgos para desarrollar acciones sobre las situaciones que están impactando o pueden impactar los resultados. Adicionalmente, el contexto de los procesos dentro de la cadena de valor permite en mayor detalle establecer escenarios de riesgo y niveles de exposición que pueden afectar el normal desarrollo de actividades y que si no se atienden pueden generar impactos mayores.

La gestión de riesgos es dinámica como lo son las organizaciones, de ahí la importancia de establecer un seguimiento estricto y periódico, así como, el análisis de datos históricos, teóricos, opiniones de expertos, necesidades de cada proceso e incluso experiencias de otras entidades.

Con todo lo anterior, el Plan Estratégico Institucional y el modelo de gestión por procesos adaptado al MIPG son elementos fundamentales para asegurar desde el inicio la debida administración de riesgos.

Los líderes de los procesos y sus equipos deben tener en cuenta toda la información relacionada con el contexto estratégico y el contexto del proceso para las etapas de identificación y valoración de los riesgos.

5.1. CONTEXTO EXTERNO E INTERNO

Se determinan las características o aspectos esenciales del entorno en el cual se encuentra la Entidad, así como, los aspectos sobre los cuales la organización busca alcanzar sus objetivos. En esta etapa se pueden observar instrumentos como el Análisis DOFA o

PESTEL y se obtienen los objetivos estratégicos y metas institucionales. En otras palabras, los elementos que constituyen el direccionamiento estratégico.

Dentro del análisis se pueden considerar los siguientes factores según corresponda:

Contexto	Factores	Descripción
Externo	Económicos	Disponibilidad de capital, liquidez, mercados financieros, desempleo, competencia
	Políticos	Cambios de Gobierno, legislación, políticas públicas, regulación
	Sociales	Demografía, responsabilidad social, orden público.
	Tecnológicos	Avances en tecnología, acceso a los sistemas de información externos, gobierno digital.
	Medio ambientales	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.
Interno	Financieros	Presupuesto de funcionamiento y de inversión, infraestructura, capacidad instalada.
	Personal	Competencia de personal, estructura organizacional, funciones, responsabilidades, rotación, disponibilidad de personal, seguridad y salud, ocupaciones, cultura organizacional-
	Tecnología	Integridad, confiabilidad, sistemas de información y seguridad de información, flujos de información y proceso para la toma de decisiones, desarrollo, mantenimientos de los sistemas de producción.
	Estratégicos	Direccionamiento Estratégico, planeación institucional, liderazgo, trabajo en equipo, políticas y objetivos estratégicos.

Fuente: Direccionamiento Estratégico

5.2. CONTEXTO POR PROCESO

Se determinan las características o aspectos esenciales del proceso y sus interrelaciones. En esta etapa se deben considerar los documentos de los procesos, su caracterización, procedimientos y todos aquellos que permiten conocer el qué, cómo, por qué y quién realiza las actividades de gestión y de control propias.

La caracterización de los procesos provee los aspectos principales que rodean al proceso, el objetivo, insumos, actividades y productos que es donde se pueden generar los riesgos que impactan la cadena de valor de la entidad.

Se pueden considerar factores como:

Factores	Descripción
Diseño del Proceso	Claridad en la descripción del objetivo y alcance del proceso.
Interacción con otros procesos	Relación con otros procesos en cuanto a insumo, proveedores, productos, usuarios y clientes.
Transversalidad	Proceso que determinan lineamientos necesarios para el desarrollo de todos los procesos.
Procedimientos documentados	La pertinencia de los procesos que se desarrollan.
Líder del proceso	Grado de responsabilidad de los funcionarios frente al proceso.
Comunicaciones entre los procesos	Efectividad de los flujos de información determinado en la interacción de los procesos.

Fuente: Modelo de Gestión por procesos

6. ESTRUCTURA PARA LA GESTIÓN DEL RIESGO

Con el fin de ejercer una correcta Administración del Riesgo, el Sanatorio de Contratación E.S.E., adoptará la metodología propuesta por el Departamento Administrativo de la Función Pública DAFP, para la presente política, el marco de referencia será la "Guía *para la Administración del Riesgo y el diseño de controles en entidades públicas, versión 6 (noviembre de 2022)*".

Para establecer los riesgos de corrupción se tendrá como referente el documento "*Estrategias para la Construcción del Plan Anticorrupción y de Atención al Ciudadano*, y la "*Guía para la Gestión del Riesgo de Corrupción*", también los lineamientos que emita la Dirección de Gestión y Desempeño Institucional del Departamento Administrativo de la Función Pública DAFP.

Para los riesgos de corrupción, en particular se deben dar reportes de los siguientes documentos establecidos por la Oficina de Control Interno del Sanatorio de Contratación E.S.E.

1. Cronograma del Plan Anticorrupción y de Atención al Ciudadano, el cual comprende un tiempo máximo para las acciones que se deben ejecutar en cada vigencia por componente e indica quienes son los responsables de cada acción.

2. Mapa de riesgos de corrupción por procesos el cual es establecido para cada vigencia, con el fin de cumplir unas acciones para mitigar los riesgos.

En lo referente a los riesgos del proceso de adquisición de bienes y servicios y en general a los riesgos en materia de contratación, se tomará como referente metodológico el Manual para la Identificación y Cobertura del Riesgo en los Procesos de Contratación de "Colombia Compra Eficiente".

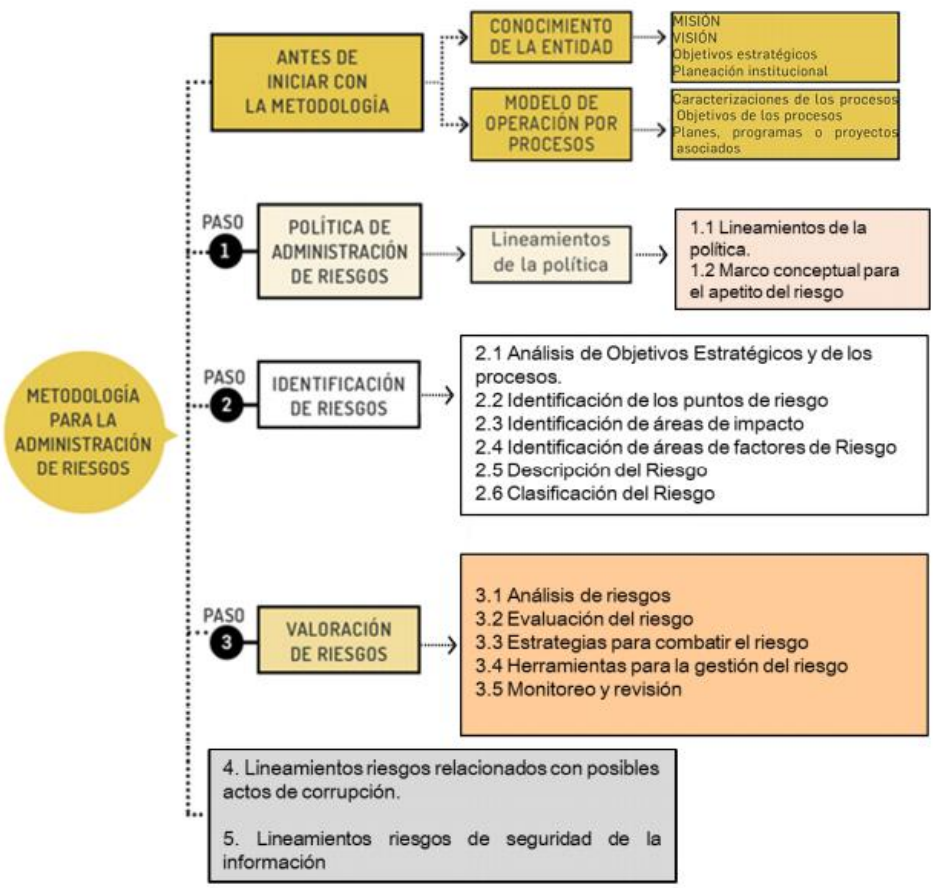
En el caso de los riesgos de seguridad digital, estos se deben gestionar de acuerdo con los criterios diferenciales descritos en el modelo de privacidad y seguridad de la información.

El resultado de aplicar la metodología propuesta será el *Mapa de Riesgos por proceso y mapa de riesgo institucional* el cual será el registro que consolidará los riesgos identificados, los recursos y acciones que se establecieron para mitigar los mismos y los responsables para ejecutarlas.

6.1. METODOLOGÍA

La metodología para la administración del riesgo requiere de un análisis inicial relacionado con el estado actual de la estructura de riesgos y su gestión en la entidad, además del conocimiento de esta desde un punto de vista estratégico de la aplicación de los tres (3) pasos básicos para su desarrollo y, finalmente, de la definición e implantación de estrategias de comunicación transversales a toda la entidad para que su efectividad pueda ser evidenciada. A continuación, se puede observar la estructura completa con sus desarrollos básicos:

Figura Metodología para la administración del riesgo



Fuente: Elaborado y actualizado por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

6.2. RESPONSABILIDAD FRENTE A LA GESTIÓN DEL RIESGO DE ACUERDO CON EL ESQUEMA DE LÍNEAS DE DEFENSA

El Modelo Integrado de Planeación y Gestión (MIPG) a través del Modelo Estándar de Control Interno (MECI) establece una estructura de control para la gestión institucional que determina los parámetros necesarios para la autogestión, la autorregulación y el autocontrol. Uno de los elementos fundamentales de esta estructura es el esquema de responsabilidades integrado por cuatro líneas de defensa el cual proporciona una manera efectiva para mejorar las comunicaciones en la gestión de los riesgos y los controles mediante la aclaración de las funciones y deberes relacionados.

En la siguiente tabla se explica la aplicación de los roles y responsabilidades del esquema de líneas de defensa para el Sanatorio de Contratación E.S.E.

Tabla. Responsabilidades de las líneas de defensa

Línea de defensa	Responsable	Responsabilidad frente a la gestión del riesgo
Línea estratégica	• La Alta Dirección de la E.S.E. (El Gerente y su Equipo Directivo) • El Comité Institucional de Coordinación de Control Interno	Definir y aprobar la Política de Administración del Riesgo, en el marco del Comité Institucional de Coordinación de Control Interno, acorde con la cual, atendiendo la periodicidad para el seguimiento a riesgos críticos debe aplicar el monitoreo correspondiente haciendo uso de la información suministrada por las instancias de 2ª línea identificadas, con base en lo cual toma las acciones necesarias para intervenir situaciones detectadas como incumplimientos, retrasos e incluso posibles actuaciones irregulares, evitando consecuencias más graves para la entidad.
Primera línea de defensa	• Lideres de procesos, programas y proyectos y sus equipos • Los servidores públicos de todos los niveles de la E.S.E.	Todos los servidores tienen una responsabilidad frente a la aplicación efectiva de los controles, por lo que se trata de un seguimiento permanente, esto incluye la aplicación de controles de gerencia operativa que corresponde a aquellos que son aplicados por

		servidores con personal a cargo (jefes, coordinadores u otro cargo).
Segunda línea de defensa	• Jefe de la Oficina de Planeación. • Comité de compras. • Encargado TIC • Responsables de temas transversales para toda la entidad y que reporta ante el Representante Legal	Hacer un seguimiento a todos los riesgos, permitiendo que se generen recomendaciones y posibles ajustes a los mapas de riesgos, de manera tal que las instancias de 1ª línea pueden establecer mejoras a los riesgos y controles, así mismo garantizar su aplicación efectiva, lo que implica que se deben incorporar ejercicios de asesoría y acompañamiento a los líderes de los procesos y sus equipos para la mejora de este tema.
Tercera línea de defensa	Oficina de Control Interno	A través de sus procesos de seguimiento y evaluación, especialmente a través de la auditoría interna deben establecer la efectividad de los controles para evitar la materialización de riesgos. De igual forma, en el marco de su Plan Anual de Auditoría puede proponer esquemas de asesoría y acompañamiento a la entidad, actividades que puede coordinar con la Oficina de Planeación.

Fuente: Basado en Guía para la Administración del Riesgo Versión 6

7. GESTIÓN DEL RIESGO

7.1. DEFINICIÓN POLÍTICA ADMINISTRACIÓN DEL RIESGO

"*El Sanatorio de Contratación Empresa Social del Estado, comprometido con el cumplimiento de su misión, visión y objetivos, implementará un Sistema de Administración de Riesgos estableciendo lineamientos precisos acerca del tratamiento, manejo, seguimiento y control a los riesgos que puedan impedir el logro de las metas institucionales y de sus procesos, contando para ello con una metodología de gestión del riesgo y personal comprometido con el mejoramiento continuo de sus procesos, quienes evaluarán la efectividad de las acciones y controles establecidos*".

7.2. IDENTIFICACIÓN DEL RIESGO

Esta etapa tiene como objetivo identificar los riesgos que estén o no bajo el control de la organización, para ello se debe tener en cuenta el contexto estratégico en el que opera la entidad, la caracterización de cada proceso que contempla su objetivo y alcance y, también, el análisis frente a los factores internos y externos que pueden generar riesgos que afecten el cumplimiento de los objetivos. Se aplican las siguientes fases:

1) **Análisis de objetivos estratégicos y de los procesos:** este paso es muy importante, dado que todos los riesgos que se identifiquen deben tener impacto en el cumplimiento del objetivo estratégico o del proceso.

2) **Identificación de los puntos de riesgo:** son actividades dentro del flujo del proceso donde existe evidencia o se tienen indicios de que pueden ocurrir eventos de riesgo operativo y deben mantenerse bajo control para asegurar que el proceso cumpla con su objetivo.

3) **Identificación de áreas de impacto:** el área de impacto es la consecuencia económica o reputacional a la cual se ve expuesta la organización en caso de materializarse un riesgo. Los impactos que aplican son **afectación económica (o presupuestal) y reputacional**.

4) **Identificación de áreas de factores de riesgo**: son las fuentes generadoras de riesgos. En la siguiente Tabla encontrará un listado con ejemplo de factores de riesgo que puede tener una entidad.

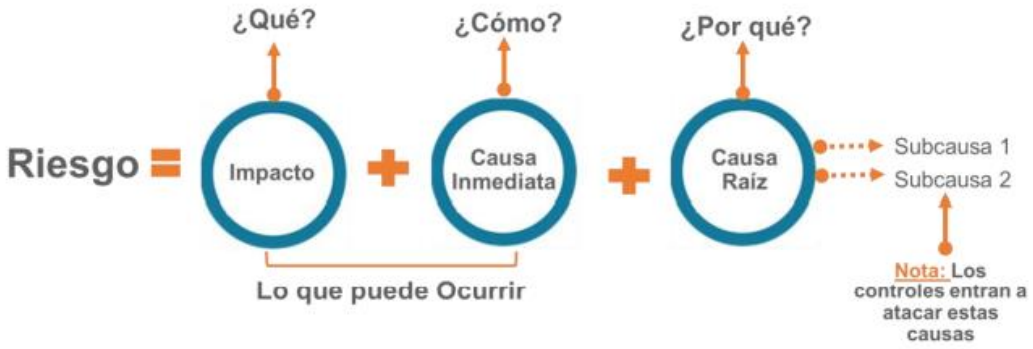
Factor	Definición		Descripción
Procesos	Eventos relacionados con errores en las actividades que deben realizar los servidores de la organización.		Falta de procedimientos
			Errores de grabación, autorización
			Errores en cálculos para pagos internos y externos
			Falta de capacitación, temas relacionados con el personal
Talento humano	Incluye seguridad y salud en el trabajo. Se analiza posible dolo e intención frente a la corrupción.		Hurto activos
			Posibles comportamientos no éticos de los empleados
			Fraude interno (corrupción, soborno)
Tecnología	Eventos relacionados con la infraestructura tecnológica de la entidad.		Daño de equipos
			Caída de aplicaciones
			Caída de redes
			Errores en programas
Infraestructura	Eventos relacionados con la infraestructura física de la entidad.		Derrumbes
			Incendios
			Inundaciones
			Daños a activos fijos

Factor	Definición		Descripción
Evento externo	Situaciones externas que afectan la entidad.		Suplantación de identidad
			Asalto a la oficina
			Atentados, vandalismo, orden público

Fuente: Adaptado del curso de riesgo Operativo de la Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de la Función Pública. 2020

5) **Descripción del riesgo:** la descripción del riesgo debe contener todos los detalles que sean necesarios y que sea fácil de entender tanto para el líder del proceso como para personas ajenas al proceso. Se propone una estructura que facilita su redacción y claridad que inicia con la frase POSIBILIDAD DE y se analizan los siguientes aspectos:

Figura Estructura propuesta para la redacción del riesgo



Fuente: Adaptado del Curso Riesgo Operativo de la Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

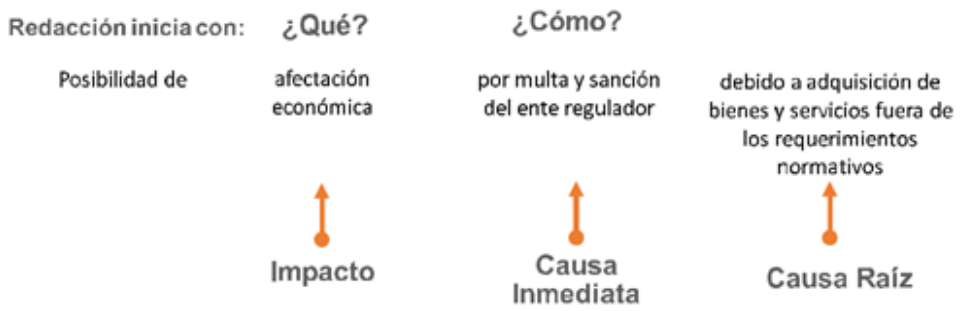
La anterior estructura evita la subjetividad en la redacción y permite entender la forma como se puede manifestar el riesgo, así como sus causas inmediatas y causas principales o raíz, esta es información esencial para la definición de controles en la etapa de valoración del riesgo. Desglosando la estructura propuesta tenemos:

- Impacto: las consecuencias que puede ocasionar a la organización la materialización del riesgo.

- Causa inmediata: circunstancias o situaciones más evidentes sobre las cuales se presenta el riesgo, las mismas no constituyen la causa principal o base para que se presente el riesgo.

- Causa raíz: es la causa principal o básica, corresponden a las razones por la cuales se puede presentar el riesgo, son la base para la definición de controles en la etapa de valoración del riesgo. Se debe tener en cuenta que para un mismo riesgo puede n existir más de una causa o subcausas que pueden ser analizadas.

Figura Ejemplo aplicado bajo la estructura propuesta para la redacción del riesgo



Fuente: Adaptado del Curso Riesgo Operativo de la Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

6) **Clasificación del riesgo:** permite agrupar los riesgos identificados, se clasifica cada uno de los riesgos en las siguientes categorías:

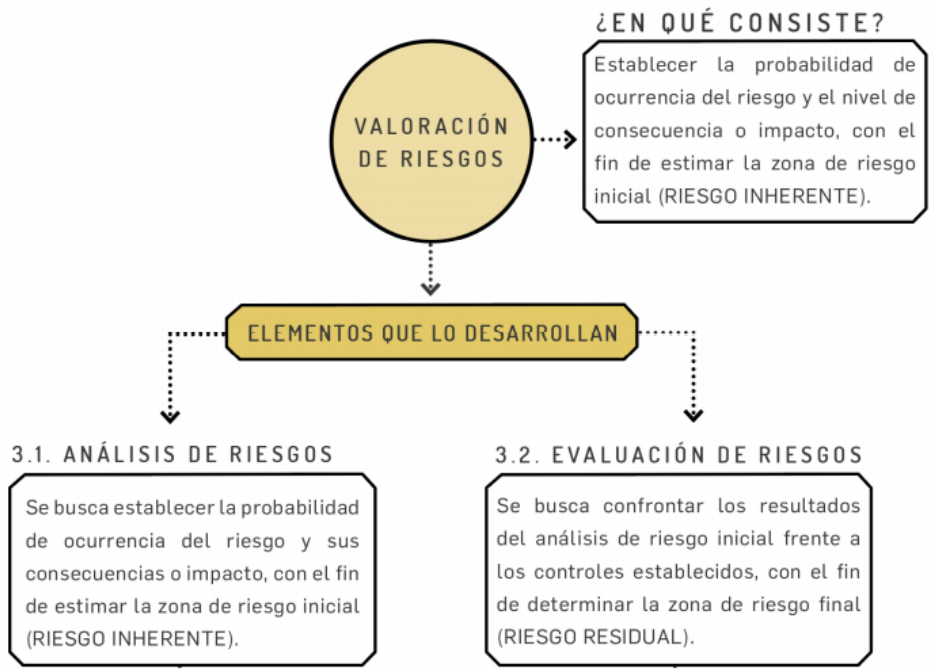
Tabla Clasificación de los riesgos

TIPO	DESCRIPCIÓN
Ejecución y administración de procesos	Pérdidas derivadas de errores en la ejecución y administración de procesos.
Fraude externo	Pérdida derivada de actos de fraude por personas ajenas a la organización (no participa personal de la entidad).
Fraude interno	Pérdida debido a actos de fraude, actuaciones irregulares, comisión de hechos delictivos abuso de confianza, apropiación indebida, incumplimiento de regulaciones legales o internas de la entidad en las cuales está involucrado por lo menos 1 participante interno de la organización, son realizadas de forma intencional y/o con ánimo de lucro para sí mismo o para terceros.
Fallas tecnológicas	Errores en hardware, software, telecomunicaciones, interrupción de servicios básicos.
Relaciones laborales	Pérdidas que surgen de acciones contrarias a las leyes o acuerdos de empleo, salud o seguridad, del pago de demandas por daños personales o de discriminación.
Usuarios, productos y prácticas	Fallas negligentes o involuntarias de las obligaciones frente a los usuarios y que impiden satisfacer una obligación profesional frente a éstos.
Daños a activos fijos/ eventos externos	Pérdida por daños o extravíos de los activos fijos por desastres naturales u otros riesgos/eventos externos como atentados, vandalismo, orden público.

Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

7.3. VALORACIÓN DEL RIESGO

El proceso de valoración del riesgo se resume en la siguiente figura:



Fuente: Dirección de Gestión y Desempeño Institucional de Función Pública, 2018.

7.3.1. Análisis de riesgos

En este punto se busca establecer la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto.

7.3.1.1. Determinar la probabilidad

Se entiende como la posibilidad de ocurrencia del riesgo. Para efectos de este análisis, la probabilidad de ocurrencia estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. De este modo, la probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año.

En la siguiente tabla se establecen los criterios para definir el nivel de probabilidad:

	Frecuencia de la Actividad	Probabilidad
Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año	20%
Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año	40%
Media	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año	60%
Alta	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5000 veces por año	80%
Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año	100%

Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

7.3.1.2. Determinar el impacto

Para la construcción de la tabla de criterios se definen los impactos económicos y reputacionales como las variables principales. Cuando se presenten ambos impactos para un riesgo, tanto económico como reputacional, con diferentes niveles se debe tomar el nivel más alto, así, por ejemplo: para un riesgo identificado se define un impacto económico en nivel insignificante e impacto reputacional en nivel moderado, se tomará el más alto, en este caso sería el nivel moderado.

En la siguiente tabla se establecen los criterios para definir el nivel de impacto.

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

Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

IMPORTANTE: Frente al análisis de probabilidad e impacto no se utiliza criterio experto, esto quiere decir que el líder del proceso, como conocedor de su quehacer, define cuántas veces desarrolla la actividad, esto para el nivel de probabilidad, y es a través de la tabla establecida que se ubica en el nivel correspondiente, dicha situación se repite para el impacto, ya que no se trata de un análisis subjetivo.

Ejemplo (continuación):

Proceso: gestión de recursos
Objetivo: adquirir con oportunidad y calidad técnica los bienes y servicios requeridos por la entidad para su continua operación.
Riesgo identificado: posibilidad de afectación económica por multa y sanción del ente regulador debido a la adquisición de bienes y servicios sin el cumplimiento de los requisitos normativos.
N.º de veces que se ejecuta la actividad: la actividad de contratos se lleva a cabo 10 veces en el mes = 120 contratos en el año.
Cálculo afectación económica: de llegar a materializarse, tendría una afectación económica de 500 SMLMV.

Aplicando las tablas de probabilidad e impacto tenemos:

	Frecuencia de la Actividad	Probabilidad
Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año	20%
Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año	40%
Media	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año	60%
Alta	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5000 veces por año	80%
Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año	100%

→ La actividad se realiza 120 veces al año, la probabilidad de ocurrencia del riesgo es **media**.

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

→ La afectación económica se calcula en 500SMLMV, el impacto del riesgo es **mayor**.

Probabilidad inherente= media 60%, **Impacto inherente:** mayor 80%

7.3.2. Evaluación de riesgos

A partir del análisis de la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto s, se busca determinar la zona de riesgo inicial (RIESGO INHERENTE).

7.3.2.1. Análisis preliminar (riesgo inherente)

Se trata de determinar los niveles de severidad a través de la combinación entre la probabilidad y el impacto. Se definen 4 zonas de severidad en la matriz de calor (ver figura Matriz de Calor).

Figura Matriz de calor (niveles de severidad del riesgo)

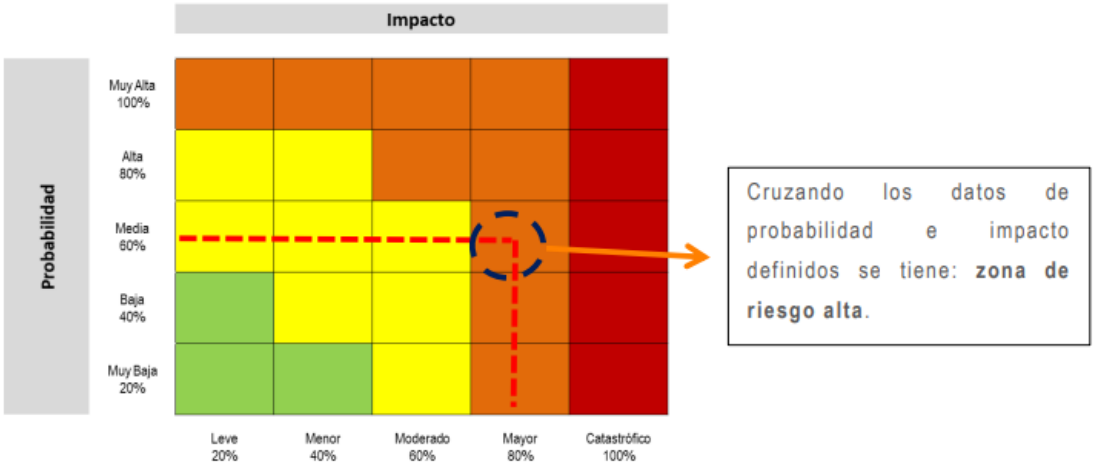
		TABLA DE SEVERIDAD				
		Impacto				
		Insignificante 20%	Menor 40%	Moderado 60%	Mayor 80%	Catastrófico 100%
Probabilidad	Muy Alto 100%	Alto	Alto	Alto	Alto	Extremo
	Alta 80%	Moderado	Moderado	Alto	Alto	Extremo
	Media 60%	Moderado	Moderado	Moderado	Alto	Extremo
	Baja 40%	Bajo	Moderado	Moderado	Alto	Extremo
	Muy Baja 20%	Bajo	Bajo	Moderado	Alto	Extremo

Fuente: Adaptado del Curso Riesgo Operativo. Universidad del Rosario. 2020.

Ejemplo (continuación):

Proceso: gestión de recursos
Objetivo: adquirir con oportunidad y calidad técnica los bienes y servicios requeridos por la entidad para su continua operación
Riesgo identificado: posibilidad de afectación económica por multa y sanción del ente regulador debido a la adquisición de bienes y servicios sin el cumplimiento de los requisitos normativos
Probabilidad Inherente: moderada 60%
Impacto Inherente: mayor 80%

Aplicando la matriz de calor, tenemos:



7.3.2.2. Valoración de controles

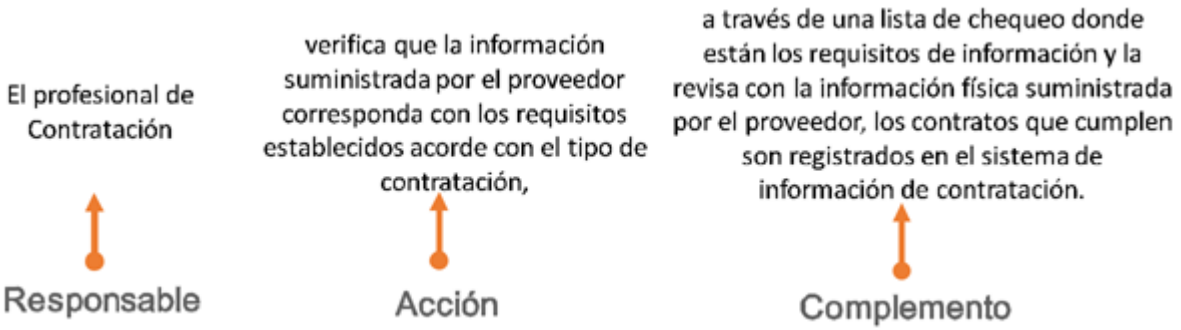
En primer lugar, conceptualmente un control se define como la medida que permite reducir o mitigar el riesgo. Para la valoración de controles se debe tener en cuenta:

- La identificación de controles se debe realizar a cada riesgo a través de las entrevistas con los líderes de procesos o servidores expertos en su quehacer. En este caso sí aplica el criterio experto.
- Los responsables de implementar y monitorear los controles son los líderes de proceso con el apoyo de su equipo de trabajo.

Estructura para la descripción del control: para una adecuada redacción del control, se establece la siguiente estructura que facilitará más adelante entender su tipología y otros atributos para su valoración:

- Responsable de ejecutar el control: identifica el cargo del servidor que ejecuta el control, en caso de que sean controles automáticos se identificará el sistema que realiza la actividad.
- Acción: se determina mediante verbos que indican la acción que deben realizar como parte del control.
- Complemento: corresponde a los detalles que permiten identificar claramente el objeto del control.

Ejemplo aplicado bajo la estructura propuesta para la redacción del control



Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

Tipología de controles y los procesos: a través del ciclo de los procesos es posible establecer cuándo se activa un control y, por lo tanto, establecer su tipología con mayor precisión.

Acorde con lo anterior, tenemos las siguientes tipologías de controles:

- Control preventivo: control accionado en la entrada del proceso y antes de que se realice la actividad originadora del riesgo, se busca establecer las condiciones que aseguren el resultado final esperado.
- Control detectivo: control accionado durante la ejecución del proceso. Estos controles detectan el riesgo, pero generan reprocesos.
- Control correctivo: control accionado en la salida del proceso y después de que se materializa el riesgo. Estos controles tienen costos implícitos.

Así mismo, de acuerdo con la forma como se ejecutan tenemos:

- Control manual: controles que son ejecutados por personas.
- Control automático: son ejecutados por un sistema.

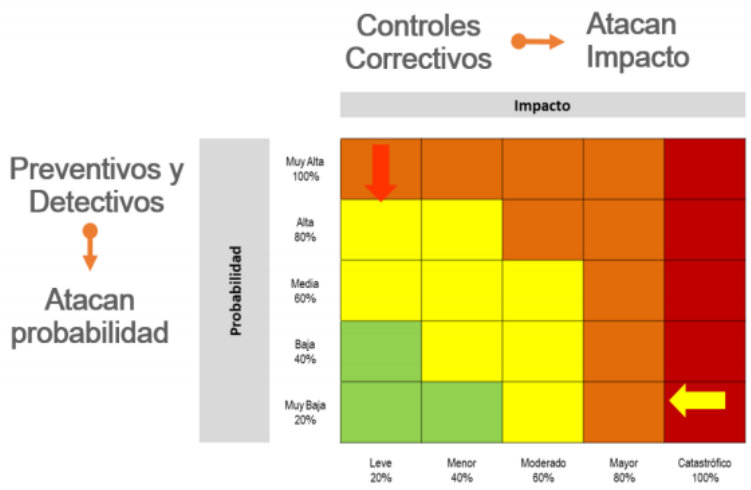
Análisis y evaluación de los controles – Atributos: A continuación, se analizan los atributos para el diseño del control, teniendo en cuenta características relacionadas con la eficiencia y la formalización. En la siguiente tabla se puede observar la descripción y peso asociados a cada uno así:

Características			Descripción	Peso
Atributos de Eficiencia	Tipo	Preventivo	Va hacia las causas del riesgo, aseguran el resultado final esperado.	25%
		Detectivo	Detecta que algo ocurre y devuelve el proceso a los controles preventivos. Se pueden generar reprocesos.	15%
		Correctivo	Dado que permiten reducir el impacto de la materialización del riesgo, tienen un costo en su implementación.	10%
	Implementación	Automático	Son actividades de procesamiento o validación de información que se ejecutan por un sistema y/o aplicativo de manera automática sin la intervención de personas para su realización.	25%
		Manual	Controles que son ejecutados por una persona., tiene implícito el error humano.	15%
*Atributos de Formalización	Documentación	Documentado	Controles que están documentados en el proceso, ya sea en manuales, procedimientos, flujogramas o cualquier otro documento propio del proceso.	-
		Sin Documentar	Identifica a los controles que pese a que se ejecutan en el proceso no se encuentran documentados en ningún documento propio del proceso	-
	Frecuencia	Continua	Este atributo identifica a los controles que se ejecutan siempre que se realiza la actividad originadora del riesgo.	-
		Aleatoria	Este atributo identifica a los controles que no siempre se ejecutan cuando se realiza la actividad originadora del riesgo	-
	Evidencia	Con Registro	Corresponde a la evidencia de la ejecución del control Ejemplo: correos electrónicos, vistos buenos y documentos electrónicos seguridad, cartas con firma mecánica, firmas digitales, actas de Juan o Comités, firma de asistencia a capacitaciones, entre otros.	-
		Sin registro	Son aquellos controles que se ejecutan, pero al validar algún tipo de evidencia de su ejecución no es posible determinarla.	-

Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

Nota: Los atributos informativos solo permiten darle formalidad al control y su fin es el de conocer el entorno del control y complementar el análisis con elementos cualitativos; sin embargo, estos no tienen una incidencia directa en su efectividad.

Teniendo en cuenta que es a partir de los controles que se dará el movimiento, en la matriz de calor se muestra cuál es el movimiento en el eje de probabilidad y en el eje de impacto de acuerdo con los tipos de controles, tal y como se muestra en la siguiente figura:



Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

Ejemplo (continuación):

Proceso: gestión de recursos
Objetivo: adquirir con oportunidad y calidad técnica los bienes y servicios requeridos por la entidad para su continua operación
Riesgo identificado: posibilidad de afectación económica por multa y sanción del ente regulador debido a la adquisición de bienes y servicios sin el cumplimiento de los requisitos normativos
Probabilidad Inherente: moderada 60%
Impacto Inherente: mayor 80%
Zona de riesgo: alta

Controles identificados:
Control 1: el profesional del área de contratos verifica que la información suministrada por el proveedor corresponda con los requisitos establecidos de contratación a través de una lista de chequeo donde están los requisitos de información y la revisión con la información física suministrada por el proveedor, los contratos que cumplen son registrados en el sistema de información de contratación.

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

En la siguiente tabla se observa la aplicación de la tabla de atributos, esta le servirá como ejemplo para el análisis y valoración de los dos controles propuestos.

Tabla Aplicación tabla atributos a ejemplo propuesto

Controles y sus características				Peso
Control 1 El profesional del área de contratos verifica que la información suministrada por el proveedor corresponda con los requisitos establecidos de contratación a través de una lista de chequeo donde están los requisitos de información y la revisión con la información física suministrada por el proveedor, los contratos que cumplen son registrados en el sistema de información de contratación.	Tipo	Preventivo	X	25%
		Detectivo		
		Correctivo		
	Implementación	Automático		
		Manual	X	15%
	Documentación	Documentado	X	-
		Sin documentar		-
	Frecuencia	Continua	X	-
		Aleatoria		-
	Evidencia	Con registro	X	-
		Sin registro		-
Total valoración control 1				**40%**
Control 2 El jefe de contratos verifica en el sistema de información de contratación la información registrada por el profesional asignado y aprueba el proceso para firma del ordenador del gasto, en el sistema de información queda el registro correspondiente, en caso de encontrar	Tipo	Preventivo		
		Detectivo	X	15%
		Correctivo		
	Implementación	Automático		
		Manual	X	15%
	Documentación	Documentado	X	-
		Sin documentar		-
	Frecuencia	Continua	X	-
		Aleatoria		-

Controles y sus características				Peso
inconsistencias, devuelve el proceso al profesional de contratos asignado.	Evidencia	Con registro	X	-
		Sin registro		-
Total valoración control 2				**30%**

Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

7.3.2.3. Nivel de riesgo (riesgo residual)

Para la aplicación de los controles se debe tener en cuenta que los estos mitigan el riesgo de forma acumulativa, esto quiere decir que una vez se aplica el valor de uno de los controles, el siguiente control se aplicará con el valor resultante luego de la aplicación del primer control.

Para mayor claridad, en la siguiente tabla se da continuación al ejemplo propuesto, donde se observan los cálculos requeridos para la aplicación de los controles.

Tabla Aplicación de controles para establecer el riesgo residual

Riesgo	Datos relacionados con la probabilidad e impacto inherentes		Datos valoración de controles		Cálculos requeridos
Posibilidad de pérdida económica por multa y sanción del ente regulador debido a la adquisición de bienes y servicios sin el cumplimiento de los requisitos normativos.	Probabilidad inherente	60%	Valoración control 1 preventivo	40%	60%* 40% = 24% 60% - 24% = **36%**
	Valor probabilidad para aplicar 2° control	36%	Valoración control 2 detectivo	30%	36%* 30% = 10,8% 36% - 10,8% = **25,2%**
	Probabilidad Residual	**25,2 %**			
	Impacto Inherente	80%			
	No se tienen controles para aplicar al impacto	N/A	N/A	N/A	N/A
	Impacto Residual	**80%**			

Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

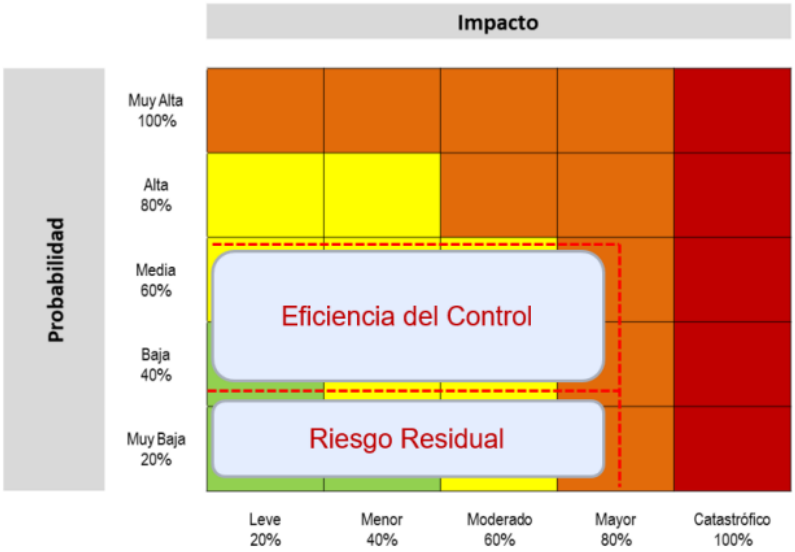
Ejemplo (continuación):

Proceso: gestión de recursos
Objetivo: adquirir con oportunidad y calidad técnica los bienes y servicios requeridos por la entidad para su continua operación
Riesgo identificado: posibilidad de afectación económica por multa y sanción del ente regulador debido a la adquisición de bienes y servicios sin el cumplimiento de los requisitos normativos
Probabilidad residual: baja 26.8%
Impacto residual: mayor 80%

Zona de riesgo residual: alta

Para este caso, si bien el riesgo se mantiene en zona alta, se bajó el nivel de probabilidad de ocurrencia del riesgo.

En la siguiente figura se observa el movimiento en la matriz de calor.



Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

Nota: En caso de no contar con controles correctivos, el impacto residual es el mismo calculado inicialmente, es importante señalar que no será posible su movimiento en la matriz para el impacto.

El Sanatorio de Contratación Empresa Social del Estado ha establecido el formato "**PL-FO-04 Mapa de Riesgos**" para el registro de los mapas de riesgo.

7.3.3. Estrategias para combatir el riesgo

Decisión que se toma frente a un determinado nivel de riesgo, dicha decisión puede ser aceptar, reducir o evitar. Se analiza frente al riesgo residual, esto para procesos en funcionamiento, cuando se trate de procesos nuevos, se procede a partir del riesgo inherente.

En la siguiente figura se observan las tres opciones mencionadas y su relación con la necesidad de definir planes de acción dentro del respectivo mapa de riesgos.

Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

Para efectos del mapa de riesgos, cuando se define la opción de reducir, se requerirá la definición de un plan de acción que especifique: i) responsable, ii) fecha de implementación, y iii) fecha de seguimiento.

Nota: El plan de acción acá referido es diferente a un plan de contingencia, el cual se enmarca en el Plan de Continuidad de Negocio[2] y se consideraría un control correctivo.

7.3.4. Herramientas para la gestión del riesgo

Como producto de la aplicación de la metodología se contará con los mapas de riesgo.

Además de esta herramienta, se tienen las siguientes:

7.3.4.1. Gestión de eventos

Un evento es un riesgo materializado, se pueden considerar incidentes que generan o podrían generar pérdidas a la entidad, se debe contar con una base histórica de eventos que permita revisar si el riesgo fue identificado y qué sucedió con los controles. En caso de que el riesgo no se hubiese identificado, se debe incluir y dar el tratamiento correspondiente

[2] De acuerdo con la Guía para la preparación de las TIC para la continuidad del negocio emitida por el Ministerio TIC lo define como procedimientos documentados que guían y orientan a las organizaciones para responder, recuperar, reanudar y restaurar la operación a un nivel predefinido de operación una vez presentada o tras la interrupción para garantizar la continuidad de las funciones críticas del negocio.

de acuerdo con la metodología. Las fuentes para establecer una base histórica de eventos son:

- Las PQRD (peticiones, quejas, reclamos, denuncias)
- Oficina jurídica
- Líneas internas de denuncia
- Comités Institucionales
- Formato de reporte de incidentes y eventos

Este mecanismo genera información para que el evento no se vuelva a presentar, así mismo, es posible establecer el desempeño de los controles así:

Desempeño del control = # eventos / frecuencia del riesgo (# veces que se hace la actividad)

7.3.4.2. Indicadores clave de riesgo

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

Tabla Ejemplos indicadores clave de riesgo

PROCESO ASOCIADO	INDICADOR	MÉTRICA
TIC	Tiempo de interrupción de aplicativos críticos en el mes	Número de horas de interrupción de aplicativos críticos al mes
FINANCIERA	Reportes emitidos al regulador fuera del tiempo establecido	Número de reportes mensuales remitidos fuera de términos
ATENCIÓN AL USUARIO	Reclamos de usuarios por incumplimiento a términos de ley o reiteraciones de solicitudes por conceptos no adecuados	% solicitudes mensuales fuera de términos % solicitudes reiteradas por tema
ADMINISTRATIVO Y FINANCIERA	Errores en transacciones y su impacto en la gestión presupuestal	Volumen de transacciones al mes sobre la capacidad disponible
TALENTO HUMANO	Rotación de personal	% de nuevos empleados que abandonan el puesto dentro de los primeros 6 meses

Fuente: Adaptado del listado de indicadores y métricas (www.riesgoscero.com) por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

7.3.5. Monitoreo y revisión

El modelo integrado de plantación y gestión (MIPG) desarrolla en la dimensión 7 control interno las líneas de defensa para identificar la responsabilidad de la gestión del riesgo y control que está distribuida en diversos servidores de la entidad.

7.3.5.1. Línea estratégica

Define el marco general para la gestión del riesgo y el control y supervisa su cumplimiento, está a cargo de la Alta Dirección y el Comité Institucional de Coordinación de Control Interno.

7.3.5.2. Primera Línea de Defensa

Desarrolla e implementa procesos de control y gestión de riesgos a través de su identificación, análisis, valoración, monitoreo y acciones de mejora.

A cargo de los gerentes públicos y líderes de programas, procesos y proyectos y de sus equipos de trabajo (en general servidores públicos en todos los niveles de la organización).

Rol principal: Diseñar, implementar y monitorear los controles y gestionar de manera directa en el día a día los riesgos de la entidad.

7.3.5.3. Segunda Línea de Defensa

Asegura que los controles y los procesos de gestión de riesgos implementados por la primera línea de defensa, estén diseñados apropiadamente y funcionen como se pretende.

A cargo de los servidores que tienen responsabilidades directas en el monitoreo y evaluación de los controles y la gestión del riesgo: Jefe de Planeación, supervisores e interventores de contratos o proyectos, coordinadores de otros sistemas de gestión de la entidad, comités de contratación, entre otros.

A continuación, se identifican los temas estratégicos y transversales relacionados con planes, programas y/o proyectos fundamentales para el cumplimiento misional de la Institución (aspectos claves de éxito):

- Plan Estratégico Institucional
- Plan de Acción Institucional
- Plan Política de Participación Social en Salud
- Plan Anual de Adquisiciones
- Plan Anticorrupción y Atención al Ciudadano
- Plan Estratégico de Talento Humano
- Plan de Bienestar e Incentivos
- Plan de Trabajo Anual en Seguridad y Salud en el Trabajo
- Plan Estratégico de Tecnologías de la Información y las Comunicaciones -- PETI
- Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información
- Plan de Seguridad y Privacidad de la Información
- Plan Institucional de Archivos de la Entidad -PINAR

Rol principal: Monitorear la gestión de riesgo y control ejecutada por la primera línea de defensa, complementando su trabajo.

7.3.5.4. Tercera Línea de Defensa

Proporciona la información sobre la efectividad del Sistema de Control Interno - SCI, a través de un enfoque basado en riesgos, incluida la operación de la primera y la segunda línea de defensa.

A cargo de la oficina de Control Interno o quien haga sus veces.

Rol principal: Proporcionar un aseguramiento basado en el más alto nivel de independencia y objetividad sobre la efectividad del SCI.

El alcance de este aseguramiento, a través de auditoría interna cubre todos los componentes del SCI.

7.4. LINEAMIENTOS PARA EL ANÁLISIS DEL RIESGO FISCAL

7.4.1. Control fiscal interno y prevención del riesgo fiscal

La construcción de este capítulo tiene como finalidad prevenir la constitución del elemento medular de la responsabilidad fiscal, que es el daño al patrimonio público, representando en el menoscabo, disminución, perjuicio, detrimento, pérdida, o deterioro de los bienes o recursos públicos, o a los intereses patrimoniales del Estado (Decreto 403, 2020, art.6).

7.4.2. Definición y elementos del riesgo fiscal

Teniendo en cuenta la estructura y elementos de la definición de riesgos que tiene la presente guía, la cual es armónica con la norma ISO 31000, se define riesgo fiscal, así:

Efecto dañoso sobre recursos públicos o bienes o intereses patrimoniales de naturaleza pública, a causa de un evento potencial.

A continuación, se describen los elementos que componen la definición de riesgo fiscal:

Efecto: es el daño que se generaría sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública, en caso de ocurrir el evento potencial.

Evento Potencial: Hechos inciertos o incertidumbres, refiriéndonos a riesgo fiscal, se relaciona con una potencial acción u omisión que podría generar daño sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública. En esta guía, el evento potencial es equivalente a la causa raíz.

Lo anterior se puede resumir de la siguiente manera:

Riesgo Fiscal = Evento Potencial (Potencial Conducta) **+** Efecto dañoso

Se debe tener especial cuidado en no confundir el riesgo fiscal, con el daño fiscal; por lo tanto, la definición debe estar orientada hacia el efecto de un evento potencial (potencial acción u omisión) sobre los recursos públicos y/o los bienes o intereses patrimoniales de naturaleza pública.

7.4.3. Metodología y paso a paso para el levantamiento del mapa de riesgos fiscales

Paso 1: identificación de riesgos fiscales

Para la identificación del riesgo fiscal es necesario establecer los puntos de riesgo fiscal y las circunstancias Inmediatas. Los puntos de riesgos son situaciones en las que potencialmente se genera riesgo fiscal, es decir, son aquellas actividades de administración, gestión, ordenación, ejecución, manejo, adquisición, planeación, conservación, custodia, explotación, enajenación, consumo, adjudicación, gasto, inversión y disposición de los bienes o recursos públicos, así como a la recaudación, manejo e inversión de sus rentas[3].

Para la identificación, se pueden usar las siguientes preguntas orientadoras:

Preguntas orientadoras para puntos riesgo fiscal y causas inmediatas

Sirve para identificar	Preguntas y respuestas para la identificación
Puntos de riesgo fiscal	¿En qué procesos de la entidad se realiza gestión fiscal? (ver capítulo inicial la definición de gestión fiscal).
Puntos de riesgo fiscal y circunstancias inmediatas	Clasifique por procesos, los hallazgos con presunta incidencia fiscal identificados por el ente de control fiscal y/o los fallos con responsabilidad fiscal en firme relacionados con hechos de la entidad o del sector y/o las advertencias de la Contraloría General de la República y/o las alertas reportadas en el Sistema de Alertas de Control Interno -SACI-. Nota 1: Para este efecto se recomienda consultar los hallazgos con presunta incidencia fiscal y los fallos con responsabilidad fiscal de los últimos 5 años. Nota 2: Los hallazgos fiscales de los últimos años y las advertencias que se hayan emitido en relación con la gestión fiscal de la entidad, se obtienen de la matriz de plan de mejoramiento institucional y de los históricos, información con la que cuenta la Oficina de Control Interno o quien haga sus veces. Nota 3: Los fallos con responsabilidad fiscal en firme son información pública, a la cual se puede acceder mediante solicitud de información y documentos (derecho de petición) ante el o los entes de control fiscal que vigilen a la entidad respectiva o al sector que esta pertenece. Estos precedentes son muy importantes para conocer las causas raíz (hechos generadores) por los que se ha fallado con responsabilidad en los últimos años y así implementar los controles adecuados para atacar de forma preventiva esas causas y evitar efectos dañosos sobre los recursos, bienes o intereses patrimoniales del Estado. Nota 4: La organización y agrupación por procesos (según el mapa de procesos de la entidad) de los hallazgos con presunta incidencia fiscal identificados por el ente de control fiscal, los fallos con responsabilidad fiscal en firme relacionados con hechos de la entidad o del sector, las advertencias de la Contraloría General de la República y las alertas reportadas en el Sistema de Alertas de Control Interno -SACI-, es una labor de la segunda línea

[3] Artículo 3 Ley 610 de 2000.

	de defensa, específicamente de la Oficinas de Planeación o quien haga sus veces, con la asesoría de la Oficina de Control Interno o quien haga sus veces.
Circunstancias inmediatas	En un ejercicio autocritico, realista y objetivo, ¿Cuáles son las causas de los hallazgos fiscales identificados por el ente de control fiscal y/o de los fallos con responsabilidad fiscal relacionados con hechos de la entidad o del sector y/o las advertencias de la oficina de control interno, en los últimos 3 años? Nota: Se recomienda no copiar las causas escritas por el órgano de control en el hallazgo, salvo que luego del análisis propio la entidad concluya que la causa del hallazgo es la identificada por el órgano de control.
Puntos de riesgo fiscal y circunstancias inmediatas	¿Qué puntos de riesgo fiscal y circunstancias inmediatas del "¿Catálogo Indicativo y Enunciativo de Puntos de riesgo fiscal y Circunstancias Inmediatas", son aplicables a la entidad?

Fuente: Elaboración Dirección de Gestión y Desempeño Institucional de Función Pública, 2022.

Identificación de las áreas de impacto

Dentro del contexto de riesgo fiscal, el área de impacto siempre corresponderá a una consecuencia económica sobre el patrimonio público, a la cual se vería expuesta la organización en caso de materializarse el riesgo.

Es importante, tener en cuenta que no todos los efectos económicos corresponden a riesgos fiscales, pero todos los riesgos fiscales (efecto dañoso sobre bienes o recursos o intereses patrimoniales de naturaleza pública) representan un efecto económico.

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

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

Otro aspecto, que es fundamental para definir de manera correcta el impacto al momento de identificar y redactar riesgos fiscales, es tener claro el concepto de patrimonio público, así como el de las tres expresiones de patrimonio público que se derivan del artículo 6 de la Ley 610 de 2000: (i) bienes públicos; recursos públicos o intereses patrimoniales de naturaleza pública (consultar definiciones en el capítulo uno de conceptos básicos).

Identificación de la causa raíz o potencial hecho generador

La causa raíz sería cualquier evento potencial (acción u omisión) que de presentarse provocaría un menoscabo, disminución, perjuicio, detrimento, pérdida o deterioro (Auditoría General de la República, 2015).

La causa raíz o potencial hecho generador y el efecto dañoso (daño) guardan entre sí una relación de causa/efecto. En este sentido, la determinación de la causa raíz o potencial hecho generador se logra estableciendo la acción u omisión o acto lesivo del patrimonio estatal.

Una adecuada gestión de riesgos fiscales exige que la identificación de causas sea especialmente objetiva y rigurosa, ya que los controles que se diseñen e implementen deben apuntarle a atacar dichas causas, para así lograr prevenir la ocurrencia de daños fiscales. Siendo la causa raíz un elemento tan relevante para la eficaz gestión de riesgos fiscales, es importante tener claridad al respecto de qué es y qué no es una causa raíz o potencial hecho generador.

Es fundamental, entonces, tener claro que debe deslindarse el hecho que ocasiona el daño (hecho generador-causa raíz o causa adecuada), del daño propiamente dicho. En otras palabras, uno es el hecho generador -causa-, y otro es el daño -efecto- (Contraloría General de la República, 2021)[4].

Ejemplo:

Una entidad X se atrasó en el pago del canon de arriendo de una de sus sedes, por 6 meses, generándose intereses moratorios por $30 millones. Cuando llega un nuevo director este encuentra la deuda por concepto de canon y los intereses generados y procede a gestionar los recursos para el pago de capital e intereses y al mes de su posesión efectúa el pago.
¿Cuál es el daño? El daño fiscal corresponde al monto pagado por concepto de intereses moratorios
¿Cuál es el hecho generador? La omisión de pagó oportuno del canon de arrendamiento.
Conclusión: El hecho generador del daño no es el pago de los intereses moratorios, ya que el pagó es una acción diligente que da cumplimiento a una obligación adquirida y evita que se sigan generando intereses.

Descripción del Riesgo Fiscal

A continuación, se presenta la estructura de redacción de riesgos fiscales en la que se conjugan los elementos antes descritos; así mismo, se presentan algunos ejemplos de riesgos fiscales identificados como resultado del estudio de fallos de contralorías territoriales y Contraloría General de la República.

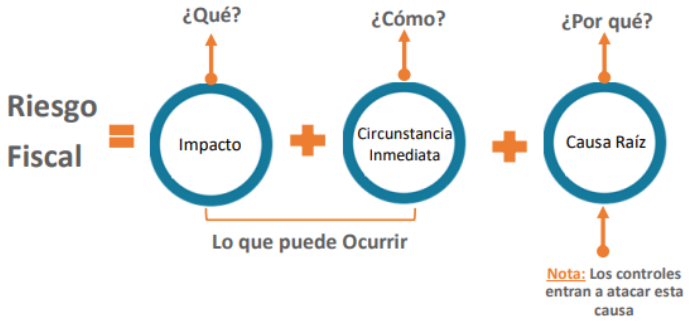
Para redactar un riesgo fiscal se debe tener en cuenta:

- ✓ Iniciar con la oración: Posibilidad de, debido a que nos estamos refiriendo al evento potencial.

[4] Concepto CGR-OJ-115 -2021 de la Contraloría General de la República, pág. 13

- ✓ Impacto: Corresponde al qué. Se refiere al efecto dañoso (potencial daño fiscal) sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública (área de impacto).
- ✓ Circunstancia inmediata: Corresponde al cómo. Se refiere a aquella situación por la que se presenta el riesgo; pero no constituye la causa principal o básica -causa raíz- para que se presente el riesgo.
- ✓ Causa Raíz: Corresponde al por qué; que es el evento (acción u omisión) que de presentarse es causante, es decir, generador directo, causa eficiente o adecuada. Es la condición necesaria, de tal forma que, si ese hecho no se produce, el daño no se genera[5].

De acuerdo con lo indicado, la estructura propuesta para la redacción de riesgos fiscales es la siguiente:



Ejemplo:

Proceso: Gestión de Recursos
Objetivo: Gestionar los bienes, obras y servicios administrativos, de mantenimiento y asistencia logística para el cumplimiento de la misión institucional.
Alcance: Inicia con la consolidación y depuración del plan de necesidades de bienes, obras y servicios que requieran los procesos institucionales en cada vigencia fiscal y culmina con el suministro de bienes y la prestación de los servicios, acorde con la disponibilidad de recursos.

[5] El control fiscal y la responsabilidad fiscal en Colombia. Luz Jimena Duque Botero y Fredy Céspedes Villa. Ibáñez 2018

¿Qué?	¿Cómo?	¿Por qué?
Posibilidad de efectos dañoso sobre **bienes públicos**	por pérdida, extravío o hurto de bienes muebles de la entidad.	a causa de la omisión en la aplicación del procedimiento para el ingreso y salida de bienes del almacén

Como complemento a continuación se muestran otros ejemplos de redacción de riesgos fiscales, según el objeto sobre el cual recae la posibilidad de efecto dañoso, es decir efecto dañoso sobre bienes públicos, recursos públicos o sobre intereses patrimoniales de naturaleza pública.

Ejemplos adicionales acorde con el objeto sobre el que recae el efecto dañoso

Bienes Públicos	Recursos públicos	Intereses patrimoniales de naturaleza pública
Posibilidad de efecto dañoso sobre bienes públicos, por daño en equipos tecnológicos, a causa de la omisión en la aplicación de medidas de prevención frente a posibles sobrecargas eléctricas.	Posibilidad de efecto dañoso sobre los recursos públicos, por pago de multa impuesta por la autoridad ambiental, a causa de la omisión en el cumplimiento de la licencia ambiental de los proyectos de infraestructura.	Posibilidad de efecto dañoso sobre intereses patrimoniales de naturaleza pública, por no tener incluidos todos los bienes muebles e inmuebles de la entidad en el contrato de seguro, a causa de la omisión en la actualización de bienes que cubren de dicho contrato.
Posibilidad de efecto dañoso sobre bienes públicos, por daño en equipos tecnológicos, a causa de la omisión en la aplicación de medidas de prevención frente a posibles sobrecargas eléctricas.	Posibilidad de efecto dañoso sobre recursos públicos, por sobrecostos en contratos de la entidad, a causa de la omisión del deber de elaborar estudios de mercado.	Posibilidad de efecto dañoso sobre intereses patrimoniales de naturaleza pública, por no devolución al tesoro público de los rendimientos financieros generados por recursos de anticipo, a causa de la omisión por parte de la interventoría y/o supervisión de la interventoría al no exigir la devolución al contratista.

Fuente: Elaboración Dirección de Gestión y Desempeño Institucional de Función Pública, 2022.

Paso 2: Valoración del riesgo fiscal

Evaluación de riesgos

Se busca establecer la probabilidad inherente de ocurrencia del riesgo fiscal y sus consecuencias o impacto inherentes.

Probabilidad

La probabilidad es la posibilidad de ocurrencia del riesgo fiscal, se determina según al número de veces que se pasa por el punto de riesgo fiscal en el periodo de 1 año, es decir, el número de veces que se realizan las actividades que representen gestión fiscal. Aplicar lo establecido en el numeral 7.3.1.1. del presente manual.

Impacto

Considerando la naturaleza y alcance del riesgo fiscal, éste siempre tendrá un impacto económico, toda vez que el efecto dañoso siempre ha de recaer sobre un bien, recurso o interés patrimonial de naturaleza pública. Aplicar lo establecido en el numeral 7.3.1.2. del presente manual.

Determinación del nivel de riesgo inherente

A partir del análisis de la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto, se busca determinar la zona de riesgo inicial (riesgo inherente), se trata de determinar los niveles de severidad, para lo cual se aplica la matriz definida en el numeral 7.3.2.1. del presente manual.

Ejemplo (continuación):

Proceso: Gestión de recursos
Objetivo: Gestionar los bienes, obras y servicios administrativos, de mantenimiento y asistencia logística para el cumplimiento de la misión institucional.
Alcance: Inicia con la consolidación y depuración del plan de necesidades de bienes, obras y servicios que requieran los procesos institucionales en cada vigencia fiscal y culmina con el suministro de bienes y la prestación de los servicios, acorde con la disponibilidad de recursos.
Punto de Riesgo: Ingreso, custodia y salida de bienes muebles de la entidad
Riesgo Fiscal: Posibilidad de efectos dañoso sobre bienes públicos (área de impacto), por pérdida, extravío o hurto de bienes muebles de la entidad (circunstancia inmediata), a causa de la omisión en la aplicación del procedimiento para el ingreso, custodia y salida de bienes e inventario del almacén y el reporte de información a quien gestiona las pólizas cuando haya lugar (causa raíz).
Probabilidad: Las veces que se pasa por el punto de riesgo en un año es 365, puesto que todos los días del año de debe ejercer la custodia de los bienes muebles de la entidad. Para este ejemplo es importante tener en cuenta que los bienes muebles en cada entidad varía en cantidad y son de distinto valor en el inventario, se sugiere analizar el tipo de bien y el

número de estos, a fin de acotar el nivel de probabilidad con un análisis más ácido que permita establecer controles diferenciados acorde con la naturaleza de diferentes grupos de bienes, ejemplo: equipos de cómputo, muebles y enseres, entre otros.

Aplicando las tablas de probabilidad e impacto tenemos:

	Frecuencia de la Actividad	Probabilidad
Muy Baja	La actividad se realiza máximo 4 veces por año.	20%
Baja	La actividad se realiza mínimo 5 veces al año y máximo 12 veces al año.	40%
Moderada	La actividad se realiza mínimo 13 veces al año y máximo 365 veces al año.	60%
Alta	La actividad se realiza mínimo 365 veces al año y máximo 3660 veces al año.	80%
Muy Alta	La actividad se realiza 3661 veces o más al año	100%

La actividad se realiza 365 veces al año, la probabilidad de ocurrencia del riesgo es **media**.

Para determinar el impacto es necesario cuantificar el potencial efecto dañoso sobre el bien, recurso o interés patrimonial de naturaleza pública.

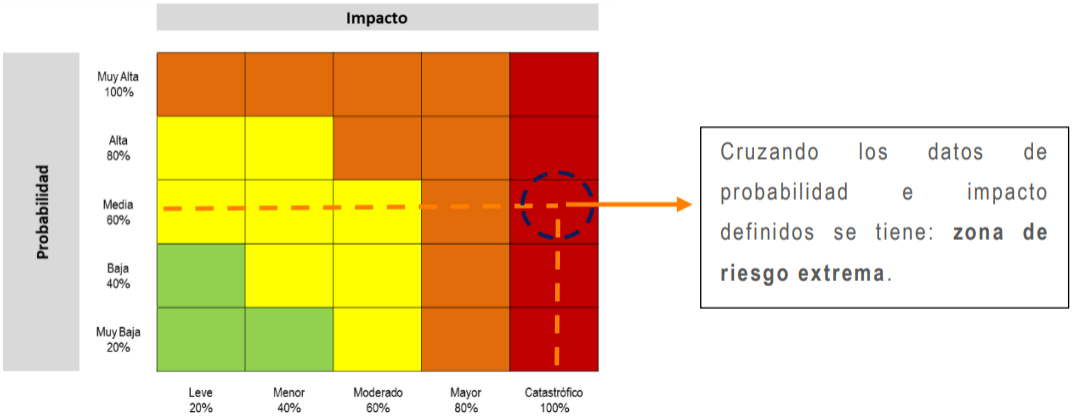
En este ejemplo el efecto dañoso sería del valor contable del inventario de bienes muebles que para el ejemplo se determina que es de $2.500 millones de pesos, lo cual corresponde a 2.500 SMLMV. De acuerdo con la tabla para la definición del nivel de impacto, este riesgo tiene un nivel de impacto catastrófico.

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

La afectación económica se calcula en más de 500SMLMV, el impacto del riesgo es **catastrófico**.

Probabilidad inherente= media 60%, **Impacto inherente:** catastrófico 100%

Zona de severidad o nivel de riesgo: De acuerdo con la tabla para la definición de zona severidad, al conjugar la calificación de probabilidad con la de impacto nos resulta un nivel de riesgo extremo.



Paso 3. Valoración de controles

Como medio para propiciar el logro de los objetivos, las actividades de control se orientan a prevenir y detectar la materialización de los riesgos.

Tipologías de controles:

- ✓ Control Preventivo: Control accionado en la entrada del proceso y antes de que se realice la actividad en la que potencialmente se origina el riesgo fiscal (punto de riesgo). Estos controles buscan establecer las condiciones que aseguren atacar la causa raíz y así evitar que el riesgo se concrete.
- ✓ Control Detectivo: Control accionado durante la ejecución de la actividad en la que potencialmente se origina el riesgo fiscal (punto de riesgo). Estos controles detectan el riesgo fiscal, pero generan reprocesos.
- ✓ Control Correctivo: Control accionado en la salida de la actividad en la que potencialmente se origina el riesgo fiscal (punto de riesgo) y después de que se materializa el riesgo fiscal. Estos controles tienen costos implícitos.

Para el análisis y evaluación de los controles se analizan los atributos para el diseño del control, teniendo en cuenta características relacionadas con la eficiencia y la formalización. Se aplican los lineamientos para la redacción del control establecidos en el numeral 7.3.2.3. del presente manual.

Ejemplo (continuación):

Proceso: Gestión de recursos
Objetivo: Gestionar los bienes, obras y servicios administrativos, de mantenimiento y asistencia logística para el cumplimiento de la misión institucional.
Alcance: Inicia con la consolidación y depuración del plan de necesidades de bienes, obras y servicios que requieran los procesos institucionales en cada vigencia fiscal y culmina con el suministro de bienes y la prestación de los servicios, acorde con la disponibilidad de recursos.

Punto de Riesgo: Ingreso, custodia y salida de bienes muebles de la entidad
Riesgo Fiscal: Posibilidad de efectos dañoso sobre bienes públicos (área de impacto), por pérdida, extravío o hurto de bienes muebles de la entidad (circunstancia inmediata), a causa de la omisión en la aplicación del procedimiento para el ingreso, custodia y salida de bienes e inventario del almacén y el reporte de información a quien gestiona las pólizas cuando haya lugar (causa raíz).
Probabilidad Inherente: Media 60%
Impacto Inherente: Catastrófico 100%
Zona de riesgo: Extrema

Controles Identificados:

✓ **Control 1 Preventivo:** El jefe de almacén valida y registra diariamente las entradas y salidas en el aplicativo dispuesto para tal fin, el cual alimenta automáticamente el inventario de bienes muebles de la entidad y su responsable.
✓ **Control 2 Detectivo:** El coordinador administrativo verifica mensualmente la relación de ingreso y salida de bienes muebles contra los inventarios generados por el sistema (actualización y ubicación en el inventario), en caso de encontrar inconsistencias solicita al jefe de Almacén ubicar el bien faltante y realizar el ajuste, teniendo en cuenta los soportes de salida e ingreso del almacén.
✓ **Control 3 Correctivo:** El director administrativo verifica la vigencia y actualización de la póliza de acuerdo con los bienes que ingresan a la entidad, en caso de presentarse un siniestro adelanta las reclamaciones respectivas ante el asegurador

Aplicando la tabla de valoración de controles tenemos:

Control 1	Criterios de efectividad			Peso
El jefe de almacén valida y registra diariamente las entradas y salidas en el aplicativo dispuesto para tal fin, el cual alimenta automáticamente el inventario de bienes muebles de la entidad y su responsable.	Tipo	Preventivo	X	25%
		Detectivo		
		Correctivo		
	Implementación	Automático		
		Manual	X	15%
	Total, Valoración Control 1 =40%			
Control 2	**Criterios de efectividad**			**Peso**
El coordinador administrativo verifica mensualmente la relación de ingreso y salida de bienes muebles contra los inventarios generados por el sistema (actualización y ubicación en el inventario), en caso de encontrar inconsistencias solicita al Jefe de Almacén ubicar el bien faltante y realizar el ajuste, teniendo en cuenta los soportes de salida e ingreso del almacén.	Tipo	Preventivo		
		Detectivo	x	15%
		Correctivo		
	Implementación	Automático		
		Manual	x	15%
	Total, Valoración Control 2 = 30%			

Control 3	Criterios de efectividad			Peso
El director administrativo verifica la vigencia y actualización de la póliza de acuerdo a los bienes que ingresan a la entidad, en caso de presentarse un siniestro adelanta las reclamaciones respectivas ante el asegurador.	Tipo	Preventivo		
		Detectivo		
		Correctivo	x	10%
	Implementación	Automático		
		Manual	x	15%
	Total, Valoración Control 3 = 25%			

Teniendo en cuenta que es a partir de los controles que se dará el movimiento, en la matriz de calor que corresponde a continuación se muestra cuál es el movimiento en el eje de probabilidad y en el eje de impacto de acuerdo con los tipos de controles y su respectiva valoración, a fin de determinar el riesgo residual.

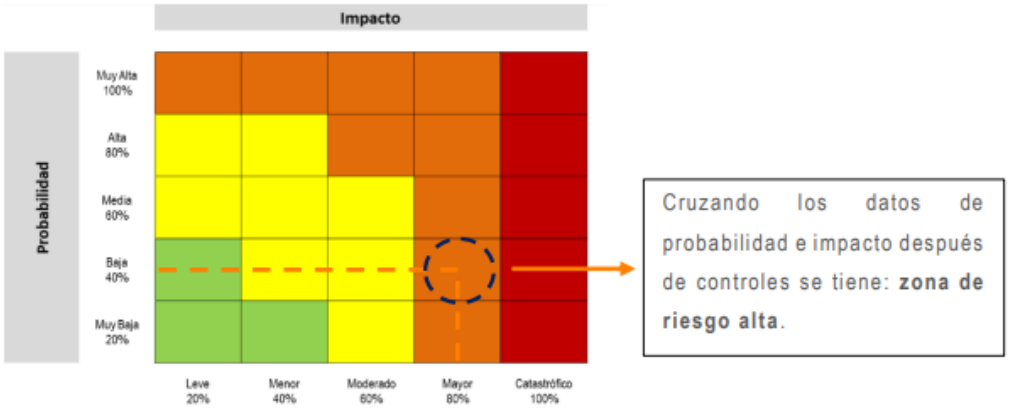
Nivel de riesgo (riesgo residual):

Es el resultado de aplicar la efectividad de los controles al riesgo inherente.

Para la aplicación de los controles se debe tener en cuenta que los estos mitigan el riesgo de forma acumulativa, esto quiere decir que una vez se aplica el valor de uno de los controles, el siguiente control se aplicará con el valor resultante luego de la aplicación del primer control. Para mayor claridad a continuación, siguiendo con el ejemplo propuesto, se observan los cálculos requeridos para la aplicación de los tres controles definidos así:

Riesgo	Datos relacionados con la probabilidad e impacto inherentes		Datos valoración de controles		Cálculos requeridos
Posibilidad de efectos dañoso sobre bienes públicos *(área de impacto)*, **por** pérdida, extravío o hurto de bienes muebles de la entidad *(circunstancia inmediata)*, **a causa de** la omisión de cumplimiento del procedimiento para el ingreso, custodia y salida de bienes e inventario del almacén y el reporte de información a quien gestiona las pólizas cuando haya lugar *(causa raiz)*.	Probabilidad Inherente	60%	Valoración control 1 preventivo	40%	60%* 40% =24% 60% - 24% = **36%**
	Valor probabilidad para aplicar 2o control	**36%**	Valoración control 2 Detectivo	30%	36%* 30% =10.8% 36% - 10,8% = **25,2%**
	Probabilidad Residual	**25,2%**			
	Impacto Inherente	100%	Valoración control correctivo	25%	100%* 25% =25% 100% - 25% = 75%
	Impacto Residual	**75%**			

Teniendo en cuenta que es a partir de los controles que se dará el movimiento, en la matriz de calor, a continuación, se muestra cuál es el movimiento en el eje de probabilidad y en el eje de impacto de acuerdo con los tipos de controles y cálculo final:



La anterior información puede trasladarse a la matriz mapa de riesgo (Formato PL-FO-04).

7.5. LINEAMIENTOS RIESGOS RELACIONADOS CON POSIBLES ACTOS DE CORRUPCIÓN

Para la gestión de riesgos de corrupción, continúan vigentes los lineamientos contenidos en la versión 4 de la Guía para la administración del riesgo y el diseño de controles en entidades públicas de 2018. Por lo anterior es necesario que, para formular el mapa de riesgos de corrupción, se remita a dicho documento. Para mayor facilidad, A continuación, se transcriben algunos de las pautas señaladas en la Guía para la administración del riesgo y el diseño de controles en entidades públicas de 2018.

7.5.1. Definición de riesgo de corrupción

Es la posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.

“Esto implica que las prácticas corruptas son realizadas por actores públicos y/o privados con poder e incidencia en la toma de decisiones y la administración de los bienes públicos” (Conpes N° 167 de 2013).

Es necesario que en la descripción del riesgo concurran los componentes de su definición, así:

ACCIÓN U OMISIÓN + USO DEL PODER + DESVIACIÓN DE LA GESTIÓN DE LO PÚBLICO + EL BENEFICIO PRIVADO

Los riesgos de corrupción se establecen sobre procesos.

El riesgo debe estar descrito de manera clara y precisa. Su redacción no debe dar lugar a ambigüedades o confusiones con la causa generadora de los mismos.

Con el fin de facilitar la identificación de riesgos de corrupción y evitar que se presenten confusiones entre un riesgo de gestión y uno de corrupción, se sugiere la utilización de la matriz de definición de riesgo de corrupción, que incorpora cada uno de los componentes de su definición.

De acuerdo con la siguiente matriz, si se marca con una X en la descripción del riesgo que aparece en cada casilla quiere decir que se trata de un riesgo de corrupción:

MATRIZ: DEFINICIÓN DEL RIESGO DE CORRUPCIÓN				
Descripción del riesgo	**Acción u omisión**	**Uso del poder**	**Desviar la gestión de lo público**	**Beneficio privado**
Posibilidad de recibir o solicitar cualquier dádiva o beneficio a nombre propio o de terceros con el fin de celebrar un contrato.	X	X	X	X

Fuente: Secretaría de Transparencia de la Presidencia de la República

7.5.2. Generalidades acerca de los riesgos de corrupción

- Se elabora anualmente por cada responsable de proceso junto con su equipo.

- Consolidación: le corresponde a la oficina de planeación, liderar el proceso de administración de los riesgos de corrupción. Adicionalmente, esta misma oficina será la encargada de consolidar el mapa de riesgos de corrupción.

- Publicación del mapa de riesgos de corrupción: se debe publicar en la página web de la entidad, en la sección de transparencia y acceso a la información pública que establece el artículo 2.1.1.2.1.4 del Decreto 1081 de 2015 o en un medio de fácil acceso al ciudadano, a más tardar el 31 de enero de cada año.

  La publicación será parcial y fundamentada en la elaboración del índice de información clasificada y reservada. En dicho instrumento la entidad debe establecer las condiciones de reserva y clasificación de algunos de los elementos constitutivos del mapa de riesgos en los términos dados en los artículos 18 y 19 de la Ley 1712 de 2014.

En este caso se deberá anonimizar esa información. Es decir, la parte clasificada o reservada, aunque se elabora, no se hace visible en la publicación.

Las excepciones solo pueden estar establecidas en la ley, un decreto con fuerza de ley o un tratado internacional ratificado por el Congreso o en la Constitución.

- Socialización: Los servidores públicos y contratistas de la entidad deben conocer el mapa de riesgos de corrupción antes de su publicación. Para lograr este propósito la oficina de planeación deberá diseñar y poner en marcha las actividades o mecanismos necesarios para que los funcionarios y contratistas conozcan, debatan y formulen sus apreciaciones y propuestas sobre el proyecto del mapa de riesgos de corrupción. Así mismo, dicha oficina adelantará las acciones para que la ciudadanía y los interesados externos conozcan y manifiesten sus consideraciones y sugerencias sobre el proyecto del mapa de riesgos de corrupción. Deberá dejarse la evidencia del proceso de socialización y publicarse sus resultados.

- Ajustes y modificaciones: se podrán llevar a cabo los ajustes y modificaciones necesarias orientadas a mejorar el mapa de riesgos de corrupción después de su publicación y durante el respectivo año de vigencia. En este caso deberán dejarse por escrito los ajustes, modificaciones o inclusiones realizadas.

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

7.5.3. Valoración de riesgos

7.5.3.1. Análisis de la probabilidad

Se analiza qué tan posible es que ocurra el riesgo, se expresa en términos de frecuencia o factibilidad, donde frecuencia implica analizar el número de eventos en un periodo determinado, se trata de hechos que se han materializado o se cuenta con un historial de situaciones o eventos asociados al riesgo; factibilidad implica analizar la presencia de factores internos y externos que pueden propiciar el riesgo, se trata en este caso de un hecho que no se ha presentado, pero es posible que suceda.

Tabla criterios de probabilidad riesgos corrupción

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

Fuente: DAFP

7.5.3.2. Análisis del impacto

El impacto se debe analizar y calificar a partir de las consecuencias identificadas en la fase de descripción del riesgo.

Tabla criterios para calificar el impacto en riesgos de corrupción

N.°	PREGUNTA: SI EL RIESGO DE CORRUPCIÓN SE MATERIALIZA PODRÍA...	RESPUESTA	
		SÍ	NO
1	¿Afectar al grupo de funcionarios del proceso?	X	
2	¿Afectar el cumplimiento de metas y objetivos de la dependencia?	X	
3	¿Afectar el cumplimiento de misión de la entidad?	X	
4	¿Afectar el cumplimiento de la misión del sector al que pertenece la entidad?		X
5	¿Generar pérdida de confianza de la entidad, afectando su reputación?	X	
6	¿Generar pérdida de recursos económicos?	X	
7	¿Afectar la generación de los productos o la prestación de servicios?	X	
8	¿Dar lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien, servicios o recursos públicos?		X
9	¿Generar pérdida de información de la entidad?		X
10	¿Generar intervención de los órganos de control, de la Fiscalía u otro ente?	X	
11	¿Dar lugar a procesos sancionatorios?	X	
12	¿Dar lugar a procesos disciplinarios?	X	
13	¿Dar lugar a procesos fiscales?	X	
14	¿Dar lugar a procesos penales?		X
15	¿Generar pérdida de credibilidad del sector?		X
16	¿Ocasionar lesiones físicas o pérdida de vidas humanas?		X
17	¿Afectar la imagen regional?		X
18	¿Afectar la imagen nacional?		X
19	¿Generar daño ambiental?		X
Responder afirmativamente de UNA a CINCO pregunta(s) genera un impacto moderado. Responder afirmativamente de SEIS a ONCE preguntas genera un impacto mayor. Responder afirmativamente de DOCE a DIECINUEVE preguntas genera un impacto catastrófico.		10	
MODERADO	Genera medianas consecuencias sobre la entidad		
MAYOR	Genera altas consecuencias sobre la entidad.		
CATASTRÓFICO :	Genera consecuencias desastrosas para la entidad		

Nivel de impacto MAYOR

Fuente: Secretaría de Transparencia de la Presidencia de la República

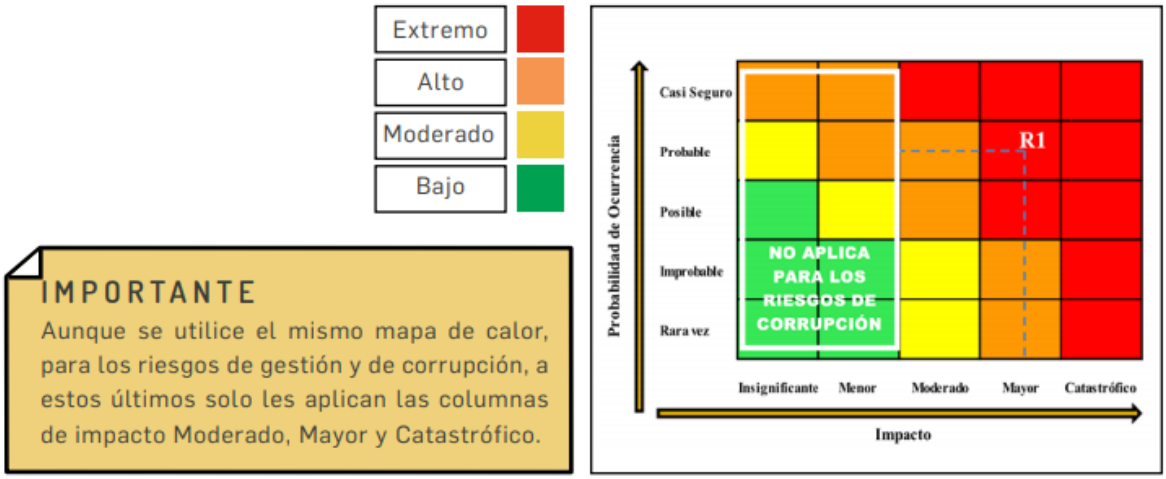
IMPORTANTE: Si la respuesta a la pregunta 16 es afirmativa, el riesgo se considera catastrófico.

Por cada riesgo de corrupción identificado, se debe diligenciar una tabla de estas.

Para los riesgos de corrupción, el análisis de impacto se realizará teniendo en cuenta solamente los niveles “moderado”, “mayor” y “catastró fico”, dado que estos riesgos siempre serán significativos; en este orden de ideas, no aplican los niveles de impacto insignificante y menor, que sí aplican para los demás riesgos.

Por último, ubique en el mapa de calor el punto de intersección resultante de la probabilidad y el impacto para establecer el nivel del riesgo inherente.

Tabla mapa de calor riesgos de corrupción



Fuente: Secretaría de Transparencia de la Presidencia de la República

7.5.3.3. Valoración de los controles – diseño de controles

Para el diseño de controles, los parámetros señalados en la versión 4 de la Guía para la administración del riesgo y el diseño de controles en entidades públicas, de 2018, continúan vigentes, por lo tanto, es necesario remitirse a dicho documento.

7.5.3.4. Nivel del riesgo (riesgo residual)

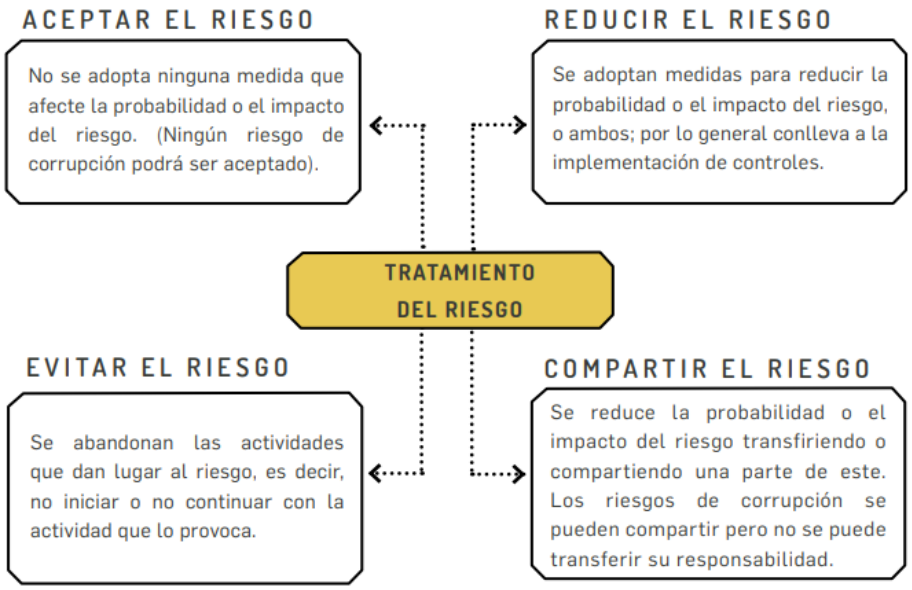
IMPORTANTE: Tratándose de riesgos de corrupción únicamente hay disminución de probabilidad. Es decir, para el impacto no opera el desplazamiento.

7.5.3.5. Tratamiento del riesgo

Es la respuesta establecida por la primera línea de defensa para la mitigación de los diferentes riesgos, incluyendo aquellos relacionados con la corrupción. A la hora de evaluar las opciones existentes en materia de tratamiento del riesgo, y partiendo de lo que establezca la política de administración del riesgo, los dueños de los procesos tendrán en cuenta la importancia del riesgo, lo cual incluye el efecto que puede tener sobre la entidad, la probabilidad e impacto de este y la relación costo-beneficio de las medidas de

tratamiento. Pero en caso de que una respuesta ante el riesgo derive en un riesgo residual que supere los niveles aceptables para la dirección se deberá volver a analizar y revisar dicho tratamiento. En todos los casos para los riesgos de corrupción la respuesta será evitar, compartir o reducir el riesgo. El tratamiento o respuesta dada al riesgo, se enmarca en las siguientes categorías:

Tabla tratamiento riesgo de corrupción



Fuente: DAFP

Como medio para propiciar el logro de los objetivos, las actividades de control se orientan a prevenir y detectar la materialización de los riesgos. Por consiguiente, su efectividad depende, de qué tanto se están logrando los objetivos estratégicos y de proceso de la entidad. Le corresponde a la primera línea de defensa el establecimiento de actividades de control.

7.5.3.6. Monitoreo de riesgos de corrupción

El gerente del Sanatorio de Contratación E.S.E., y los líderes de los procesos, en conjunto con sus equipos, deben monitorear y revisar periódicamente la gestión de riesgos de corrupción y si es el caso ajustarlo (primera línea de defensa).

Le corresponde, igualmente, a la oficina de planeación adelantar el monitoreo (segunda línea de defensa), para este propósito se sugiere elaborar una matriz. Dicho monitoreo será en los tiempos que determine la entidad.

Su importancia radica en la necesidad de llevar a cabo un seguimiento constante a la gestión del riesgo y a la efectividad de los controles establecidos. Teniendo en cuenta que la corrupción es, por sus propias características, una actividad difícil de detectar.

Para tal efecto deben atender a los lineamientos y las actividades descritas en la primera y segunda línea de defensa de este documento.

7.5.3.7. Reporte de la gestión del riesgo de corrupción

De igual forma, se debe reportar en el mapa y plan de tratamiento de riesgos los riesgos de corrupción, de tal manera que se comunique toda la información necesaria para su comprensión y tratamiento adecuado.

7.5.3.8. Seguimiento de riesgos de corrupción

- Seguimiento: El Jefe de Control Interno o quien haga sus veces, debe adelantar seguimiento al Mapa de Riesgos de Corrupción. En este sentido es necesario que adelante seguimiento a la gestión del riesgo, verificando la efectividad de los controles.
- Primer seguimiento: Con corte al 30 de abril. En esa medida, la publicación deberá surtirse dentro de los diez (10) primeros días del mes de mayo.
- Segundo seguimiento: Con corte al 31 de agosto. La publicación deberá surtirse dentro de los diez (10) primeros días del mes de septiembre.
- Tercer seguimiento: Con corte al 31 de diciembre. La publicación deberá surtirse dentro de los diez (10) primeros días del mes de enero.
- El seguimiento adelantado por la Oficina de Control Interno se deberá publicar en la página web de la entidad o en un lugar de fácil acceso para el ciudadano.
- Verificar la publicación del Mapa de Riesgos de Corrupción en la página web de la entidad.
- Seguimiento a la gestión del riesgo.
- Revisión de los riesgos y su evolución.
- Asegurar que los controles sean efectivos, le apunten al riesgo y estén funcionando en forma adecuada.

7.5.3.9. Acciones en caso de materialización de riesgos de corrupción

En el evento de materializarse un riesgo de corrupción, es necesario realizar los ajustes necesarios con acciones, tales como:

1) Informar a las autoridades de la ocurrencia del hecho de corrupción.
2) Revisar el mapa de riesgos de corrupción, en particular, las causas, riesgos y controles.
3) Verificar si se tomaron las acciones y se actualizó el mapa de riesgos de corrupción.
4) Llevar a cabo un monitoreo permanente.

La Oficina de Control Interno debe asegurar que los controles sean efectivos, le apunten al riesgo y estén funcionando en forma oportuna y efectiva. Las acciones adelantadas se refieren a:

- Determinar la efectividad de los controles.
- Mejorar la valoración de los riesgos.
- Mejorar los controles.
- Analizar el diseño e idoneidad de los controles y si son adecuados para prevenir o mitigar los riesgos de corrupción.
- Determinar si se adelantaron acciones de monitoreo.
- Revisar las acciones del monitoreo.

7.6. LINEAMIENTOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Se debe tener en cuenta que la política de seguridad digital se vincula al modelo de seguridad y privacidad de la información (MSPI), el cual se encuentra alineado con el marco de referencia de arquitectura TI y soporta transversalmente los otros habilitadores de la política de gobierno digital: seguridad de la información, arquitectura, servicios ciudadanos digitales.

7.6.1. Identificación de los activos de seguridad de la información

Como primer paso para la identificación de riesgos de seguridad de la información es necesario identificar los activos de información del proceso.

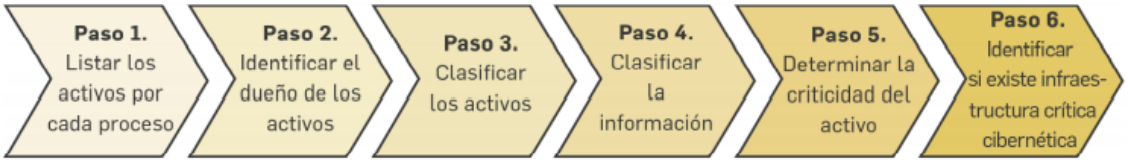
¿Qué son los activos de la información? Un activo es cualquier elemento que tenga valor para la organización, sin embargo, en el contexto de seguridad digital, son activos elementos tales como: -Aplicaciones de la organización.

¿Por qué identificar los activos? Permite determinar qué es lo más importante que la entidad y sus procesos poseen (sean bases de datos, archivos, servidores web o aplicaciones clave para que la entidad pueda prestar sus servicios).

¿Qué son los activos? Servicios web, Redes, Información física o digital, Tecnologías de información TI, Tecnologías de operación TO que utiliza la organización para funcionar en el entorno digital.

¿Por qué identificar los activos de la información? La entidad puede saber qué es lo que debe proteger para garantizar tanto su funcionamiento interno como su funcionamiento de cara al ciudadano, aumentando así su confianza en el uso del entorno digital.

Pasos para la identificación de activos



Fuente: Elaboración conjunta entre la Dirección de Gestión y Desempeño Institucional de Función Pública y el Ministerio TIC, 2018.

Nota: para realizar la identificación de activos deberá remitirse a la sección 3.1.6 del anexo 4 "Modelo nacional de gestión de riesgo de seguridad de la información en entidades públicas".

Tabla ejemplo identificación activos del proceso

Proceso	Activo	Descripción	Dueño del activo	Tipo del activo	Ley 1712 de 2014	Ley 1581 de 2012	Criticidad respecto a su confidencialidad	Criticidad respecto a completitud o integridad	Criticidad respecto a su disponibilidad	Nivel de criticidad
Gestión financiera	Base de datos de nómina	Base de datos con información de nómina de la entidad	Jefe de oficina financiera	Información	Información reservada	No contiene datos personales	ALTA	ALTA	ALTA	ALTA
Gestión financiera	Aplicativo de nómina	Servidor web que contiene el *front office* de la entidad	Jefe de oficina financiera	Software	N/A	N/A	BAJA	MEDIA	BAJA	MEDIA
Gestión financiera	Cuentas de cobro	Formatos de cobro diligenciados	Jefe de oficina financiera	Información	Información pública	No contiene datos personales	BAJA	BAJA	BAJA	BAJA

Fuente: Ministerio de Tecnologías de la Información y Comunicaciones Min TIC, 2018.

7.6.2. Identificación del riesgo

Se podrán identificar los siguientes tres (3) riesgos inherentes de seguridad de la información:

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

Para cada riesgo se deben asociar el grupo de activos, o activos específicos del proceso, y conjuntamente analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización. Para este efecto, es necesario consultar el Anexo 4 Modelo nacional de

gestión de riesgos de seguridad de la información para entidades públicas donde se encuentran las siguientes tablas necesarias para este análisis:

- Tabla 5. Tabla de amenazas comunes
- Tabla 6. Tabla de amenazas dirigida por el hombre
- Tabla 7. Tabla de vulnerabilidades comunes

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

Tabla de amenazas y vulnerabilidades de acuerdo con el tipo de activo

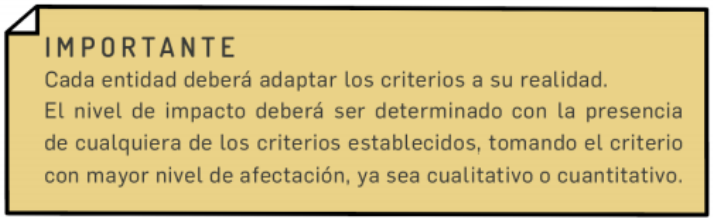
Tipo de activo	Ejemplos de vulnerabilidades	Ejemplos de vulnerabilidades
Hardware	Almacenamiento de medios sin protección	Hurto de medios o documentos
Software	Ausencia de parches de seguridad	Abuso de los derechos
Red	Líneas de comunicación sin protección	Escucha encubierta
Información	Falta de controles de acceso físico	Hurto de información
Personal	Falta de capacitación en las herramientas	Error en el uso
Organización	Ausencia de políticas de seguridad	Abuso de los derechos

Fuente: Ministerio de Tecnologías de la Información y Comunicaciones Min T IC, 2018.

7.6.3. Valoración del riesgo

Para esta etapa se utilizarán las tablas de probabilidad e impacto definidas en los numerales 5.3.1.1. y 5.3.1.2. del presente manual.

Para el análisis preliminar (riesgo inherente), en esta etapa se define el nivel de severidad para el riesgo de seguridad de la información identificado, para ello, se aplica la matriz de calor establecida en el numeral 5.3.2.1. del presente manual.



Las variables confidencialidad, integridad y disponibilidad se definen de acuerdo con el modelo de seguridad y privacidad de la información de la estrategia de Gobierno Digital (GD) del Ministerio de Tecnologías de la Información y las Comunicaciones.

La variable población se define teniendo en cuenta el establecimiento del contexto externo de la entidad, es decir, que la consideración de población va a estar asociada a las personas a las cuales se les prestan servicios o trámites en el entorno digital y que de una u otra forma pueden verse afectadas por la materialización de algún riesgo en los activos identificados. Los porcentajes en las escalas pueden variar, según la entidad y su contexto.

La variable presupuesto es la consideración de presupuesto afectado por la entidad debido a la materialización del riesgo, contempla sanciones económicas o impactos directos en la ejecución presupuestal.

La variable ambiental estará también alineada con la afectación del medio ambiente por la materialización de un riesgo de seguridad digital. Esta variable puede no ser utilizada en la mayoría de los casos, pero debe tenerse en cuenta, ya que en alguna eventualidad puede existir afectación ambiental.

Figura Valoración del riesgo en seguridad de la información

RIESGO	ACTIVO	AMENAZA	VULNERABILI-DAD	PROBABILIDAD	IMPACTO	ZONA DE RIESGO
Pérdida de la Confiden-cialidad	Base de datos de nómina	Modificación no autorizada	Ausencia de políticas de control de acceso	4-Probable	**4- Mayor**	**Extrema**
			Contraseñas sin protección			
			Ausencia de mecanismos de identificación y autenticación de usuarios			
			Ausencia de bloqueo de sesión			

Fuente: Adaptado de Instituto de Auditores Internos. COSO ERM. Agosto 2004.

Extremo
Alto
Moderado
Bajo

IMPORTANTE:
La probabilidad y el impacto se determinan con base a la amenaza, no en las vulnerabilidades.

7.6.4. Controles asociados a la seguridad de la información

Se podrán mitigar/tratar los riesgos de seguridad de la información empleando como mínimo los controles del Anexo A de la ISO/IEC 27001:2013, estos controles se encuentran en el anexo 4. "Modelo Nacional de Gestión de riesgo de seguridad de la Información en entidades públicas", siempre y cuando se ajusten al análisis de riesgos.

Acorde con el control seleccionado, será necesario considerar las características de diseño y ejecución definidas para su valoración.

A continuación, se incluyen algunos ejemplos de controles y los dominios a los que pertenecen, la lista completa se encuentra en del documento maestro del modelo de seguridad y privacidad de la información (MSPI):

Tabla Controles para riesgos de seguridad de la información

Procedimientos operacionales y responsabilidades	Objetivo: asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información
Procedimientos de operación documentados	Control: los procedimientos de operación se deberían documentar y poner a disposición de todos los usuarios que los necesiten.
Gestión de cambios	Control: se deberían controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.
Gestión de capacidad	Control: para asegurar el desempeño requerido del sistema se debería hacer seguimiento al uso de los recursos, llevar a cabo los ajustes y las proyecciones de los requisitos sobre la capacidad futura.
Separación de los ambientes de desarrollo, pruebas y operación	Control: se deberían separar los ambientes de desarrollo, prueba y operación para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.
Protección contra códigos maliciosos	Objetivo: asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.
Controles contra códigos maliciosos	Control: se deberían implementar controles de detección, prevención y recuperación, combinados con la toma de conciencia apropiada por parte de los usuarios para protegerse contra códigos maliciosos.
Copias de respaldo	Objetivo: proteger la información contra la perdida de datos.
Respaldo de información	Control: se deberían hacer copias de respaldo de la información, del software y de las imágenes de los sistemas, ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada.

Fuente: Ministerio de Tecnologías de la Información y Comunicaciones Min TIC 2018.

Figura Formato mapa riesgos seguridad de la información

N.	RIESGO	ACTIVO	TIPO	AMENAZAS	TIPO	PROBABILIDAD	IMPACTO	RIESGO RESIDUAL	OPCIÓN TRATAMIENTO	ACTIVIDAD DE CONTROL	SOPORTE	RESPONSABLE	TIEMPO	INDICADOR
2	**Pérdida de la integridad**	Base de datos de nómina	Seguridad digital	Modificación no autorizada	Ausencia de políticas de control de acceso	**Probable**	**Menor**	**Moderado**	Reducir	A.9.1.1 Política de control de acceso	Política creada y comunicada	Oficina TI	Tercer trimestre de 2018	**EFICACIA:** Índice de cumplimiento actividades= (# de actividades cumplidas / # de actividades programadas) x 100 **EFECTIVIDAD:** Efectividad del plan de manejo de riesgos= (# de modificaciones no autorizadas)
					Contraseñas sin protección				Reducir	A.9.4.3 Sistema de gestión de contraseñas	Procedimientos para la gestión y protección de contraseñas	Oficina TI	Tercer trimestre de 2018	
					Ausencia de mecanismos de identificación y autenticación de usuarios				Reducir	A 9.4.2 Procedimiento de ingreso seguro	Procedimiento para ingreso seguro	Oficina TI	Tercer trimestre de 2018	
					"Ausencia de bloqueo				Reducir	A.11.2.8 Equipos de usuario desatendidos	Configuraciones para bloqueo automático de sesión	Oficina TI	Tercer trimestre de 2018	

*En este ejemplo el responsable de las actividades de control fue la Oficina de TI, sin embargo existen actividades para el área de personal, recursos físicos o cada oficina en particular. El análisis de riesgos determinará los controles y los responsables en cada caso.

Fuente: Elaboración conjunta entre la Dirección de Gestión y Desempeño Institucional de Función Pública y el Ministerio TIC, 2018.

8. PERIODICIDAD DE REVISIÓN Y AJUSTE

La Política y el Manual de Administración del Riesgo, será sujeto de revisión, ajuste y/o actualización de acuerdo con las directrices del Departamento Administrativo de la Función Pública y/o a las necesidades del Sanatorio de Contratación Empresa Social del Estado.

9. CONTROL DE CAMBIOS

VERSIÓN	FECHA	ELABORADO POR	REVISADO POR	APROBADO POR	OBSERVACIONES
1	23/06/2021	Alvaro Gamboa Rojas Encargado de Calidad	Comité Coordinador de Control Interno	Acta No. 003- 2021 Comité Institucional de Gestión y Desempeño	Creación del documento.
2	30/08/2023	Alvaro Gamboa Rojas Encargado de Calidad	Comité Coordinador de Control Interno	Acta No. 003- 2023 Comité Institucional de Gestión y Desempeño	Creación del documento.

REFERENCIAS

Guía para la administración del riesgo y el diseño de controles en entidades públicas. Versión 6. Dirección de Gestión y Desempeño Institucional. Noviembre de 2022.