INTRODUCCIÓN

La Unidad de Información y Análisis Financiero –UIAF-, es una unidad administrativa especial, adscrita al Ministerio de Hacienda y Crédito Público, cuyas funciones son las de intervenir en la economía del Estado mediante actividades de inteligencia financiera, a fin de detectar y prevenir el lavado de activos, la financiación del terrorismo, operaciones sospechosas de comercio exterior, que puedan tener relación directa o indirecta con actividades de contrabando y fraude aduanero (Leyes 526 de 1999, 1121 de 2006 y 1762 de 2015).

El concepto de Administración del Riesgo se introduce en las entidades públicas, teniendo en cuenta que todas las organizaciones independientemente de su naturaleza, tamaño y razón de ser están permanentemente expuestas a diferentes riesgos o eventos que pueden poner en peligro su existencia.

Para la Unidad de Información y Análisis Financiero - UIAF, la administración de riesgos es fundamental para asegurar el cumplimiento de la misión institucional y de los objetivos trazados dentro del Sistema Integrado de Gestión.

La administración del Riesgo comprende el conjunto de Elementos de Control y sus interrelaciones, para que la institución evalúe e intervenga aquellos eventos, tanto internos como externos, que puedan afectar de manera positiva o negativa el logro de sus objetivos institucionales. La administración del riesgo contribuye a que la entidad consolide su Sistema de Control Interno y a que se genere una cultura de Autocontrol y autoevaluación al interior de la misma.

Teniendo en cuenta que los riesgos son posibilidades de ocurrencia de toda situación que pueda desviar el normal desarrollo de las actividades de los procesos e impidan el logro de los objetivos estratégicos para el cumplimiento de la misión institucional, la Unidad de Información y Análisis Financiero - UIAF está fortaleciendo su Proceso Estratégico, de acuerdo con los lineamientos del Modelo Estándar de Control Interno – MECI, y en particular, el Componente de Administración de Riesgos, a través del análisis y estructuración de los elementos de control definidos en el Sistema Integral de Gestión.

Para contar con una adecuada administración de los riesgos, se hace necesario definir criterios orientadores respecto al tratamiento de los riesgos identificados a fin de mitigar sus efectos en la entidad, elementos que están contendidos dentro de la presente política, con los cuales se pretende en primera instancia, transmitir el enfoque de la alta dirección sobre la manera de abordar la administración de los riesgos institucionales, socializar con todos los funcionarios un lenguaje común sobre este tema y difundir las políticas formuladas que permitan la sostenibilidad del sistema de administración de riesgos.

Las políticas identifican las opciones para tratar y manejar los riesgos basadas en la valoración de los mismos, permiten tomar decisiones adecuadas y fijar los lineamientos, que van a transmitir la posición de la dirección y establecen las guías de acción necesarias a todos los servidores de la entidad.

El presente documento comprende la definición de la política y las acciones institucionales a emprender, que permita encausar el accionar de la entidad hacia el uso eficiente de los recursos y la continuidad en la prestación de los servicios con calidad.

1. OBJETIVO

Establecer los lineamientos y criterios que orienten a la Unidad de Información y Análisis Financiero - UIAF en la identificación, valoración, tratamiento, monitoreo y seguimiento a los riesgos (de gestión, de corrupción, de seguridad digital, de fraude, de conflicto de interés) y potenciales eventos de pérdida de continuidad del negocio, que puedan impactar de manera negativa en el cumplimiento de la misión y el logro de los objetivos institucionales, fortaleciendo el esquema de prevención y control a partir de los niveles de responsabilidad y autoridad establecidas por el modelo de líneas de defensa a través de la Política de Control Interno del MIPG.

2. ALCANCE

La presente política es aplicable a todos los planes, programas, proyectos y procesos del modelo de operación de la entidad, junto con las actividades que se deriven de los mismos y ejecutadas por los servidores públicos durante el ejercicio de sus funciones. Así mismo, es de obligatorio cumplimiento por los responsables definidos en este documento incluyendo los respectivos compromisos en el plan de acción de las áreas involucradas.

3. MARCO NORMATIVO

- Constitución Política de Colombia de 1991, a través de la cual se adopta los principios de la función administrativa y elimina el control fiscal previo y obligatoriedad para todas las entidades estatales de contar con el control interno;
- Literal a) del Artículo 2° de la Ley 87 de 1993 – Objetivos del Control Interno. Proteger los recursos de la organización, buscando su adecuada administración ante posibles riesgos que los afectan;
- Literal f) del Artículo 2° de la Ley 87 de 1993 – Objetivos del Control Interno. 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, a través de la cual se fortalece el Control Interno, mediante la creación del Sistema Nacional de Control Interno;
- Artículo 4° del Decreto 1537 de 2001 "Por el cual se reglamenta parcialmente la Ley 87 de 1993 en cuanto a elementos técnicos y administrativos que fortalezcan el sistema de control interno de las entidades y organismos del Estado" – 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 organizacionales, 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 1599 de 2005, mediante el cual se adopta un marco general para el ejercicio del Control Interno, a través del Modelo Estándar de Control Interno –MECI y dota al Estado colombiano de una estructura única;

- Artículo 73 de la Ley 1474 de 2011 "Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública" – Plan Anticorrupción y de Atención al Ciudadano. "Cada entidad del orden nacional, departamental y municipal deberá elaborar anualmente una estrategia de lucha contra la corrupción y de atención al ciudadano. Dicha estrategia contemplará, entre otras cosas, el mapa de riesgos de corrupción en la respectiva entidad, las medidas concretas para mitigar esos riesgos, las estrategias antitrámites y los mecanismos para mejorar la atención al ciudadano. …";
- Decreto 943 de 2014 "Por el cual se actualiza el Modelo Estándar de Control Interno (MECI)";
- Numeral 1.3 del Manual Técnico del Modelo Estándar de Control Interno para el Estado Colombiano MECI 2014. Componente Administración del Riesgo. "Las políticas identifican las opciones para tratar y manejar los riesgos basadas en la valoración de los mismos, permiten tomar decisiones adecuadas y fijar los lineamientos, que van a transmitir la posición de la dirección y establecen las guías de acción necesarias a todos los servidores de la entidad. Es importante que las Políticas de Administración del Riesgo se fijen desde el inicio del proceso, dado que estos, deberán someterse a los lineamientos y directrices que en esta etapa se determinen";
- Decreto 1443 de 2014 "Por el cual se dictan disposiciones para la implementación del Sistema de Gestión de la Seguridad y Salud en el Trabajo (SG-SST)";
- Artículo 133 de la Ley 1753 de 2015, por medio de la cual se integra en un solo Sistema de Gestión, los Sistemas de Gestión de la Calidad (Ley 872 de 2003) y de Desarrollo Administrativo (Ley 489 de 1998) articulado con los Sistemas Nacional e Institucional de Control Interno (Ley 87 de 1993 y en los artículos 27 al 29 de la Ley 489 de 1998);
- 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". Articula el Sistema de Gestión en el marco del Modelo Integrado de Planeación y Gestión – MIPG, a través de los mecanismos de control y verificación que permiten el cumplimiento de los objetivos y el logro de resultados de las entidades. Actualiza el Modelo Estándar de Control Interno para el Estado Colombiano – MECI a través del Manual Operativo del Modelo Integrado de Planeación y Gestión – MIPG (correspondiendo a la 7° Dimensión de MIPG);
- Decreto 648 de 2018 "Por el cual se modifica y adiciona el Decreto 1083 de 2015, Reglamentario Único del Sector de la Función Pública. 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 612 de 2018 "Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado"
- Resolución interna 228 de octubre 18 de 2017 "Por la cual se deroga la Resolución 182 de 2016 y los artículos tercero y cuarto de la Resolución 099 de 2017, y se crea y conforma el Comité Institucional de Gestión y Desempeño de la Unidad de Información y Análisis Financiero – UIAF";
- Decreto 1008 de 2018 "Por el cual se establecen los lineamientos generales de la política de gobierno digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del decreto 1078 del 2015, decreto único reglamentario del sector de tecnologías de la información y las telecomunicaciones".
- Resolución 257 de noviembre 11 de 2018 "Por la cual se unifica en una sola resolución las Resoluciones No. 041 de fecha 15 de junio de 2000, No. 007 de fecha 30 de marzo de 2001, No. 172 de 2008 y 277 de 2017, sobre creación, integración y funcionamiento del Comité de Coordinación del Sistema de Control Interno de la Unidad de Información y Análisis Financiero UIAF y se incluyen modificaciones legales y reglamentarias";
- Guía para la administración del riesgo y el diseño de controles en entidades públicas. Versión 5. Diciembre de 2020.

4. TÉRMINOS Y DEFINICIONES

- **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.
- **Administración de Riesgos**: proceso efectuado por la Alta Dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos. El enfoque de riesgos no se determina solamente con el uso de la metodología, sino logrando que la evaluación de los riesgos se convierta en una parte natural del proceso de planeación.
- **Alta Dirección:** persona o grupo de personas del máximo nivel jerárquico que dirigen y controlan una entidad.
- **Amenaza:** medida que modifica el riesgo (procesos, políticas, dispositivos, prácticas u otras acciones).
- **Análisis de Riesgo:** elemento de control que permite establecer la probabilidad de ocurrencia de los eventos positivos y/o negativos y el impacto de sus consecuencias, calificándolos y evaluándolos a fin de determinar la capacidad de la entidad pública para su aceptación y manejo. Se debe llevar a cabo un uso sistemático de la información disponible para determinar qué tan frecuentemente pueden ocurrir eventos especificados y la magnitud de sus consecuencias.
- **Apetito del 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 (Tomado de la Guía para la administración del Riesgo y el diseño de controles en entidades públicas - Versión 5).
- **Autoevaluación del Control:** elemento de control que, basado en un conjunto de mecanismos de verificación y evaluación, determina la calidad y efectividad de los controles internos a nivel de los procesos y de cada área organizacional responsable, permitiendo emprender las acciones de mejoramiento del control requeridas. Se basa en una revisión periódica y sistemática de los procesos de la entidad para asegurar que los controles establecidos son aún eficaces y apropiados.
- **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 (Tomado de la Guía para la administración del Riesgo y el diseño de controles en entidades públicas - Versión 5).
- **Causa:** todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo (Tomado de la Guía para la administración del Riesgo y el diseño de controles en entidades públicas - Versión 5).
- **Causa Inmediata:** circunstancias bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo (Tomado de la Guía para la administración del Riesgo y el diseño de controles en entidades públicas - Versión 5).
- **Causa Raíz:** causa principal o básica, corresponde a las razones por la cuales se puede presentar el riesgo (Tomado de la Guía para la administración del Riesgo y el diseño de controles en entidades públicas - Versión 5).
- **Compartir el Riesgo:** se asocia con la forma de protección para disminuir las pérdidas que ocurran luego de la materialización de un riesgo, es posible realizarlo mediante contratos, seguros, cláusulas contractuales u otros medios que puedan aplicarse.
- **Confidencialidad:** propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados (Tomado de la Guía para la administración del Riesgo y el diseño de controles en entidades públicas - Versión 5).
- **Conflicto de Intereses:** en Colombia, el concepto conflicto de intereses se encuentra definido en el artículo 40 del Código Único Disciplinario –Ley 734 de 2002– y el artículo 11 del Código de Procedimiento

Administrativo y de lo Contencioso Administrativo – Ley 1437 de 2011 –, los cuales señalan que el conflicto surge "cuando el interés general propio de la función pública entra en conflicto con el interés particular y directo del servidor público". La Organización para la Cooperación y el Desarrollo Económico – OCDE, define el conflicto de intereses como "un conflicto entre las obligaciones públicas y los intereses privados de un servidor público, en el que el servidor público tiene intereses privados que podrían influir indebidamente en la actuación de sus funciones y sus responsabilidades oficiales". Para la organización Transparencia por Colombia "el conflicto de intereses surge cuando un servidor público tiene un interés privado que podría influir, o en efecto influye, en el desempeño imparcial y objetivo de sus funciones oficiales, porque le resulta particularmente conveniente a él, o a su familia, o a sus socios cercanos" (Tomado de la Guía para la identificación y declaración del conflicto de intereses en el sector público colombiano, versión 2, julio de 2019).

- **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 (Tomado de la Guía para la administración del Riesgo y el diseño de controles en entidades públicas - Versión 5).
- **Contingencia:** acción que debe seguirse al momento de materializarse el riesgo, con el fin de seguir prestando el servicio o se puedan desarrollar las operaciones con el menor traumatismo posible.
- **Control:** medida que permite reducir o mitigar un riesgo (Tomado de la Guía para la administración del Riesgo y el diseño de controles en entidades públicas - Versión 5).
- **Control Adecuado:** es el que está presente si la dirección ha planificado y organizado (diseñado) las operaciones de manera tal que proporcionen un aseguramiento razonable de que los objetivos y metas de la organización serán alcanzados de forma eficiente y económica.
- **Corrupción:** uso del poder para desviar la gestión de lo público hacia el beneficio privado.
- **Disponibilidad:** propiedad de ser accesible y utilizable a demanda por una entidad (Tomado de la Guía para la administración del Riesgo y el diseño de controles en entidades públicas - Versión 5).
- **Evaluación del Riesgo:** proceso utilizado para determinar las prioridades de la Administración del Riesgo comparando el nivel de un determinado riesgo con respecto a un estándar determinado.
- **Factores de Riesgo:** son las fuentes generadoras de riesgos (Tomado de la Guía para la administración del Riesgo y el diseño de controles en entidades públicas - Versión 5).
- **Gestión del Riesgo de Corrupción:** proceso para identificar, evaluar, manejar y controlar acontecimientos o situaciones potenciales, con el fin de proporcionar un aseguramiento razonable respecto al alcance de los objetivos de la organización.
- **Identificación del Riesgo:** elemento de control, que posibilita conocer los eventos potenciales, estén o no bajo el control de la entidad pública, que ponen en riesgo el logro de su misión, estableciendo los agentes generadores, las causas y los efectos de su ocurrencia. se puede entender como el proceso que permite determinar qué podría suceder, por qué sucedería y de qué manera se llevaría a cabo.
- **Impacto:** las consecuencias que puede ocasionar a la organización la materialización del riesgo (Tomado de la Guía para la administración del Riesgo y el diseño de controles en entidades públicas - Versión 5).
- **Integridad:** propiedad de exactitud y completitud (Tomado de la Guía para la administración del Riesgo y el diseño de controles en entidades públicas - Versión 5).
- **Mapa de Riesgo:** documento con la información resultante de la gestión del riesgo.
- **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 puede 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 (Tomado de la Guía para la administración del Riesgo y el diseño de controles en entidades públicas - Versión 5).

- **Política:** directriz emitida por la dirección sobre lo que hay que hacer para efectuar el control. Constituye la base de los procedimientos que se requieren para la implantación del control.
- **Probabilidad:** se entiende la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. La probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año (Tomado de la Guía para la administración del Riesgo y el diseño de controles en entidades públicas - Versión 5).
- **Proceso:** conjunto de actividades mutuamente relacionadas o que interactúan para generar un valor.
- **Riesgo:** efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales. Los eventos potenciales hacen referencia a la posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos (Tomado de la Guía para la administración del Riesgo y el diseño de controles en entidades públicas - Versión 5).
- **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 (Tomado de la Guía para la administración del Riesgo y el diseño de controles en entidades públicas - Versión 5).
- **Riesgo de Gestión:** posibilidad de que suceda algún evento que tendrá un impacto sobre el cumplimiento de los objetivos. Se expresa en términos de probabilidad y consecuencias.
- **Riesgo de Seguridad de la Información:** posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).
- **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 (Tomado de la Guía para la administración del Riesgo y el diseño de controles en entidades públicas - Versión 5).
- **Riesgo Residual:** el resultado de aplicar la efectividad de los controles al riesgo inherente (Tomado de la Guía para la administración del Riesgo y el diseño de controles en entidades públicas - Versión 5).
- **Tolerancia al 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 (Tomado de la Guía para la administración del Riesgo y el diseño de controles en entidades públicas - Versión 5).
- **Vulnerabilidad:** representan la debilidad de un activo o de un control que puede ser explotada por una o más amenazas (Tomado de la Guía para la administración del Riesgo y el diseño de controles en entidades públicas - Versión 5).

5. ROLES Y RESPONSABILIDADES FRENTE AL RIESGO

Con el fin de asegurar que las responsabilidades y autoridades para la gestión del riesgo se asignan y comunican a los roles pertinentes, la UIAF determina las siguientes responsabilidades de acuerdo con las líneas de Defensa establecidas en la Guía para la administración de los riesgos y diseño de controles en entidades públicas, versión 5, diciembre de 2020, DAFP.

Las líneas de defensa hacen referencia a un modelo de control que establece los roles y responsabilidades de todos los actores del riesgo y control de la entidad, proporcionando el aseguramiento de la gestión para prevenir la materialización de los riesgos en todo su ámbito[1]

[1] Guía para la administración del riesgo y el diseño de controles en entidades públicas. Riesgos de gestión, corrupción y seguridad digital. Versión 4. Octubre de 2018.

Líneas de Defensa	Responsables	Roles y Responsabilidades
Línea Estratégica Es una instancia decisoria dentro del Sistema de Control Interno	**Alta Dirección** (Equipo Directivo) **Comité Institucional de Coordinación de Control Interno** (Director General, Subdirectores, Jefes de Oficina) **Comité Institucional de Gestión y Desempeño** (Director General, Subdirectores, Jefes de Oficina)	**a. Roles y Responsabilidades**
		1. Definir y aprobar el marco general para la gestión del riesgo, la gestión para la continuidad del negocio y el control; 2. Analizar los riesgos, vulnerabilidades, amenazas y escenarios de pérdida de continuidad de negocio institucionales que puedan afectar el cumplimiento de los objetivos estratégicos, planes institucionales, metas, compromisos y capacidades para prestar sus servicios.
		b. Actividades a Realizar
		1. Fortalecer el Comité Institucional de Coordinación de Control Interno, incrementando su periodicidad para las reuniones, 2. Definir y aprobar y la política de administración del riesgo, 3. Definir los niveles de aceptación del riesgo, 4. Establecer la periodicidad del monitoreo y seguimiento, 5. Supervisar el cumplimiento de cada una de las etapas de la administración del riesgo, 6. Revisar los cambios en el Direccionamiento Estratégico y en el entorno y cómo estos pueden generar nuevos riesgos o modificar los existentes, 7. Revisar los planes de acción establecidos en los riesgos materializados, a fin de que se tomen medidas oportunas y eficaces para evitar su posible repetición, 8. Evaluar la forma como funciona el Esquema de Líneas de Defensa, 9. Realizar la evaluación de la Política de Administración del Riesgo, considerando su aplicación, cambios en el entorno, dificultades para su desarrollo y riesgos emergentes, 10. Realizar la evaluación de la Política de Gestión Estratégica del Talento Humano, considerando la forma de provisión de los cargos, la capacitación, código de integridad, bienestar.
		c. Comunicación y Divulgación
		1. Corresponde al Comité Institucional de Coordinación de Control Interno asegurarse de que la Política de Administración del Riesgo sea dada a conocer a todos los niveles de la entidad, que se conozcan claramente los niveles de responsabilidad y autoridad que posee cada una de las tres líneas de defensa frente a la gestión del riesgo; 2. Buscar crear conciencia en todos los servidores públicos de la entidad, sobre la importancia de la gestión preventiva y el autocontrol en la ejecución de sus actividades; 3. Divulgar y socializar la Política, Metodología y Mapa de Riesgos, incluyendo su publicación en el sitio web.
		d. Accionar ante la Materialización del Riesgo
		Revisar los planes de acción definidos en los riesgos materializados, a fin de que se tomen las medidas oportunas y eficaces para evitar la posible repetición del evento.

<table>
<tr><th>Líneas de Defensa</th><th>Responsables</th><th>Roles y Responsabilidades</th></tr>
<tr><td rowspan="8">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</td><td rowspan="8">Gerentes Públicos, Líderes de Programas, Procesos, Proyectos y de Equipos de Trabajo</td><td>a. Roles y Responsabilidades</td></tr>
<tr><td>1. Diseñar, implementar y monitorear los controles;
2. Gestionar de manera directa en el día a día los riesgos de la entidad;
3. Orientar el desarrollo e implementación de políticas y procedimientos internos y asegurar que sean compatibles con las metas y objetivos de la entidad y emprender las acciones de mejoramiento para su logro;
4. Informar a la Segunda Línea de Defensa (Oficina Asesora de Planeación o quien haga sus veces), sobre los riesgos materializados en los objetivos, programas, proyectos, procesos y planes a su cargo;
5. Asegurar que al interior de sus equipos de trabajo se reconozca el concepto de “administración del riesgo”, la política y metodología definida, los actores y el entorno de los procesos</td></tr>
<tr><td>b. Actividades a Realizar</td></tr>
<tr><td>1. Revisar los cambios en el Direccionamiento Estratégico o en el entorno y cómo estos pueden generar nuevos riesgos o modificar los existentes;
2. Liderar la identificación de los riesgos de los programas, procesos, proyectos y planes a su cargo, de acuerdo con los lineamientos establecidos en la Guía Metodológica vigentes y establecida por el DAFP;
3. Revisar el adecuado diseño y ejecución de los controles establecidos para la mitigación de riesgos;
4. Formular o actualizar los mapas de riesgos de gestión, de corrupción y de seguridad digital asociados a los diferentes programas, procesos, proyectos y planeas a su cargo;
5. Revisar el cumplimiento de los objetivos de los programas, procesos, proyectos o planes y sus indicadores de desempeño, e identificar los riesgos que se materialicen;
6. Reportar a la Oficina Asesora de Planeación o quien haga sus veces los avances y evidencias de la gestión de los riesgos, así como los eventos de riesgos que se materialicen;
7. Formular los planes de mejoramiento, su aplicación y seguimiento para resolver los hallazgos presentados;
8. Evaluar periódicamente la eficacia de los controles identificados en el proceso de caracterización de los riesgos;</td></tr>
<tr><td>c. Comunicación y Consulta</td></tr>
<tr><td>1. Asegurarse de implementar la metodología para mitigar los riesgos en la operación, reportando a la Segunda Línea sus avances y dificultades;
2. Divulgar y sensibilizar al interior de sus áreas el mapa de riesgos de sus procesos, junto con el Plan de Manejo de Riesgos y las Políticas de Operación que se hayan definido.</td></tr>
<tr><td>d. Accionar ante la Materialización del Riesgo</td></tr>
<tr><td>1. Ante el conocimiento sobre un hecho de corrupción, informar a la instancia pertinente, de acuerdo con el conducto regular establecido por la entidad y según el alcance (normatividad asociada al hecho de corrupción materializado), realizar la denuncia ante la instancia de control correspondiente;
2. Ante la materialización de riesgos de gestión, de continuidad de negocio o de seguridad digital, proceder de manera inmediata a aplicar el plan de</td></tr>
</table>

Líneas de Defensa	Responsables	Roles y Responsabilidades
		contingencia (de existir), que permita el restablecimiento del servicio (si es el caso), de acuerdo con el respectivo Plan de Mejoramiento; 3. Iniciar el análisis de causas y determinar las acciones preventivas y de mejora, documentar el Plan de Mejoramiento Institucional y verificar la calificación y ubicación del riesgo para su inclusión en el mapa de riesgos; 4. Analizar y actualizar el Mapa de Riesgos del proceso.

Líneas de Defensa	Responsables	Roles y Responsabilidades
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	**Jefes de las Oficinas Asesoras de Planeación o Quienes Hagan sus Veces,** **Supervisores e Interventores de Contratos o Proyectos,** **Coordinadores de Otros Sistemas de Gestión de la Entidad,** **Comité de Riesgos (donde existan),** **Comités de Contratación,** **Coordinadores de Equipos de Trabajo,** **Áreas Financieras,** **Áreas de TIC**	**a. Roles y Responsabilidades** 1. Monitorear la gestión de riesgo y control ejecutada por la Primera Línea de Defensa, complementando su trabajo; 2. Asegurar que los controles y procesos de gestión de riesgos implementados por la Primera Línea de Defensa, estén diseñados apropiadamente y funcionen como se pretende **b. Actividades a Realizar** 1. LA Oficina Asesora de Planeación o quien haga sus veces, define la metodología para la administración del riesgo, acorde a la normatividad y lineamientos para cada tipo de riesgo a excepción de los riesgos que por naturaleza requieran una metodología particular (Riesgos ambientales, de seguridad de la información, de continuidad del negocio y de seguridad y salud en el trabajo); 2. La Oficina Asesora de Planeación o quien haga sus veces, asesora a la Línea Estratégica en el análisis del contexto interno y externo, para la Política de Administración del Riesgo, el establecimiento de los Niveles de Impacto y el Nivel de Aceptación del Riesgo; 3. La Oficina Asesora de Planeación o quien haga sus veces, acompaña, orienta y entrena metodológicamente a los líderes de los procesos en la identificación, análisis y valoración del riesgo y la respectiva construcción del mapa de riesgos del proceso; 4. La Oficina Asesora de Planeación o quien haga sus veces, diseña, implementa y socializa la herramienta o instrumento para la caracterización de los riesgos institucionales; 5. La Oficina Asesora de Planeación o quien haga sus veces, adelanta el monitoreo de los mapas de riesgos, evaluando la eficacia de los controles y los cambios de valoración del riesgo residual que se presenten en el ejercicio de la gestión del riesgo; 6. La Oficina Asesora de Planeación o quien haga sus veces, consolida y publica los mapas de riesgos, de acuerdo con los lineamientos normativos; 7. Revisar los cambios en el Direccionamiento Estratégico y el entorno y cómo esos pueden generar nuevos riesgos o modificar los que ya se tienen identificados en cada uno de los procesos, para solicitar y apoyar en la actualización de los mapas de riesgos; 8. Revisar la adecuada definición de los objetivos institucionales y de los procesos y realizar las recomendaciones a que haya lugar; 9. Revisar el adecuado diseño de los controles para la mitigación de los riesgos que se han establecido por la Primera Línea de Defensa y realizar

Líneas de Defensa	Responsables	Roles y Responsabilidades
		las recomendaciones y seguimiento para el fortalecimiento de los mismos; 10. Revisar el perfil de riesgo inherente y residual para cada proceso y el consolidado y advertir sobre cualquier riesgo que esté por fuera del perfil de riesgo de la entidad; 11. Realizar el seguimiento para que las actividades de control establecidas para la mitigación de los riesgos de los procesos se encuentren documentadas y actualizadas en los procedimientos; 12. Revisar los planes de acción establecidos para cada uno de los riesgos materializados, con el fin de que se tomen las medidas oportunas y eficaces para evitar en lo posible que se vuelva a materializar el riesgo; 13. Realizar el monitoreo a los riesgos con la periodicidad establecida; 14. Los Líderes de Proceso, realizan autoevaluación a la administración del riesgo y hacer seguimiento a la ejecución de controles y determinación de materialización de riesgos; 15. Los supervisores e interventores de contratos acompañan a los líderes de los procesos en la identificación, análisis y valoración del riesgo y definición de controles en los temas a su cargo y con enfoque en la prevención.
		c. Comunicación y Consulta
		1. Difundir y asesorar a la Primera Línea de Defensa en la metodología, así como de los Planes de Tratamiento de Riesgos identificados en todos los niveles de la entidad, de tal forma que se asegure su implementación; 2. Impulsar a nivel institucional una cultura de gestión del riesgo, a través de capacitaciones, mesas de trabajo y asesorías, con el fin de mejorar el conocimiento y apropiación del enfoque basado en riesgos; 3. Divulgar el Mapa de Riesgos de Corrupción a las partes interesadas y comunidad en general, mediante su publicación en el sitio web.
		d. Accionar ante la Materialización del Riesgo
		1. Asesorar a la Primera Línea de Defensa en el análisis de causas y la determinación de acciones preventivas y de mejora y documentar en el Plan de Mejoramiento Institucional; 2. Revisar los planes de acción establecidos para cada uno de los riesgos materializados, con el fin de que se tomen medidas oportunas y eficaces para evitar en lo posible que se vuelva a materializar el riesgo; 3. Actualizar el mapa de riesgos, con la información reportada por la Primera Línea de Defensa.

Líneas de Defensa	Responsables	Roles y Responsabilidades
Tercera Línea de Defensa Proporciona información sobre la	**Oficina de Control Interno**	**a. Roles y Responsabilidades**
		1. Proporcionar un aseguramiento basado en el más alto nivel de independencia y objetividad sobre la efectividad del Sistema de Control Interno; 2. Proporcionar aseguramiento objetivo en las temáticas identificadas no cubiertas por la segunda línea de defensa;

Líneas de Defensa	Responsables	Roles y Responsabilidades
efectividad del Sistema de Control Interno, a través de un enfoque basado en riesgos, incluida la operación de la primera y segunda línea de defensa		3. Recomendar mejoras a las Políticas de Operación para la administración del riesgo.
		b. Actividades a Realizar
		1. Prestar asesoría de forma conjunta con la Oficina Asesora de Planeación a la primera línea de defensa, en la metodología e identificación de los riesgos y diseño de controles; 2. Evaluar que se revisen los cambios en el Direccionamiento Estratégico y en el entorno y que se identifiquen y actualicen los mapas de riesgo por parte de los responsables de los procesos; 3. Revisar que las áreas realicen una adecuada definición de los objetivos institucionales y de los objetivos de los procesos y realizar las recomendaciones a que haya lugar; 4. Revisar que se hayan identificado los riesgos significativos que pueden afectar el cumplimiento de los objetivos estratégicos y de los objetivos de los procesos; 5. Revisar el adecuado diseño y ejecución de los controles para la mitigación de los riesgos que se hayan identificado por la primera línea de defensa y realizar las recomendaciones y seguimiento para el fortalecimiento de los mismos; 6. Revisar el perfil de riesgo inherente y residual para cada proceso y realizar las observaciones y recomendaciones para aquellos que estén por fuera del perfil de riesgo de la entidad o que su calificación del impacto o probabilidad del riesgo no sea coherente con los resultados de las auditorías realizadas; 7. Realizar el seguimiento a los riesgos consolidados en los mapas de riesgo, verificando la adecuada identificación, análisis, valoración y tratamiento de los riesgos del proceso, de conformidad con el Plan Anual de Auditoría y reportar los resultados al Comité Institucional de Coordinación de Control Interno; 8. Verificar que las evidencias reportadas estén acordes con las definidas en los controles para su mitigación; 9. Revisar la efectividad de los controles y planes de acción propuestos y, de ser necesario, proponer las mejoras al mismo; 10. Publicar de acuerdo con la normatividad vigente los informes de seguimiento y de las auditorías realizadas a los mapas de riesgo; 11. Alertar a la Línea Estratégica sobre la probabilidad de ocurrencia de riesgos de corrupción en las áreas y procesos auditados; 12. Realizar las recomendaciones de mejora a la Política de Administración del Riesgo.
		c. Comunicación y Consulta
		1. Impulsar a nivel institucional una cultura de gestión del riesgo, a través de capacitaciones, mesas de trabajo y asesorías, a fin de mejorar el conocimiento y apropiación del enfoque basado en riesgos;

Líneas de Defensa	Responsables	Roles y Responsabilidades
		2. Presentar el informe de la gestión de la entidad, a través de un enfoque basado en riesgos, incluyendo la operación de la primera y segunda línea de defensa.
		d. Accionar ante la Materialización del Riesgo
		1. Informar a la Segunda Línea de Defensa, con el fin de facilitar el inicio de las acciones correspondientes con el líder del proceso; 2. Acompañar al líder del proceso en la revisión, análisis y definición de las acciones con el fin de que se tomen las medidas oportunas y eficaces para evitar en lo posible que se vuelva a materializar el riesgo; 3. Verificar que se hayan tomado las acciones correctivas, preventivas o de mejora y se realice la actualización del respectivo mapa de riesgo.

5.1. Responsable de Seguridad Digital:

La entidad debe designar un responsable de Seguridad Digital que también es el responsable de la Seguridad de la Información, el cual debe pertenecer a un área que haga parte de la Alta Dirección o Línea Estratégica y las responsabilidades que debe cumplir respecto a la gestión del riesgo de seguridad digital serán las siguientes:

- Definir el procedimiento para la Identificación y Valoración de Activos.
- Adoptar o adecuar el procedimiento formal para la gestión de riesgos de seguridad digital (Identificación, Análisis, Evaluación y Tratamiento).
- Asesorar y acompañar a la primera línea de defensa en la realización de la gestión de riesgos de seguridad digital y en la recomendación de controles para mitigar los riesgos.
- Apoyar en el seguimiento a los planes de tratamiento de riesgo definidos.
- Informar a la línea estratégica sobre cualquier variación importante en los niveles o valoraciones de los riesgos de seguridad digital.
- Las demás definidas en la Guía de Roles y Responsabilidades del Modelo de Seguridad y Privacidad de la Información – MSPI.

6. POLÍTICA

La Unidad de Información y Análisis Financiero - UIAF se compromete a establecer y mantener acciones efectivas con la participación de todos los servidores públicos de la entidad encaminadas a reducir la posibilidad de materialización de las situaciones de amenaza de aquellos eventos internos o externos que puedan afectar el logro de los objetivos institucionales, la calidad de sus productos y servicios y el cumplimiento de su misión y visión.

6.1. Tipo de Política

De acuerdo con el 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”, esta política institucional, se articula con la Política de Direccionamiento Estratégico y Planeación del Modelo Integrado de Planeación y Gestión – MIPG II.

7. ALINEACIÓN DE LA POLÍTICA DE ADMINISTRACIÓN DEL RIESGO CON LA PLATAFORMA ESTRATÉGICA DE LA ENTIDAD

La Unidad de Información y Análisis Financiero – UIAF, fue creada por la Ley 526 del 12 de agosto de 1999, reglamentada parcialmente por el Decreto 1497 de 2002 y modificada por la Ley 1121 del 29 de diciembre de 2006, como una unidad administrativa especial adscrita al Ministerio de Hacienda y Crédito Público, cuya función principal es la de intervenir en la economía del Estado, mediante actividades de inteligencia financiera, a fin de detectar y prevenir el lavado de activos, la financiación del terrorismo, operaciones sospechosas de comercio exterior, que puedan tener relación directa o indirecta con actividades de contrabando y fraude aduanero.

Como parte de su misionalidad, la UIAF ha establecido una plataforma estratégica, la cual hace parte integral en la definición de los lineamientos de la administración del riesgo descritos en la presente política:

7.1. Propósito Superior:

Proteger la economía nacional y contribuir con el bienestar de los colombianos.

7.2. Misión:

Prevenir y detectar el lavado de activos y el financiamiento del terrorismo, centralizando, sistematizando y analizando información para consolidar y difundir resultados de valor estratégico con el propósito superior de proteger la economía nacional y contribuir con el bienestar de los colombianos.

7.3. Visión:

La UIF de Colombia en el 2022 será modelo líder en inteligencia económica y financiera, reconocida internacionalmente por contar con un sistema innovador, dinámico y efectivo en la prevención y detección de lavado de activos y el financiamiento del terrorismo.

7.4. Estrategias y Objetivos Estratégicos:

a. **Estrategia 1. Prioridad:** mantener los casos operacionales del lavado de activos y la financiación del terrorismo con el fin de prevenir y detectar el lavado sofisticado y sus redes conexas.
   Objetivos Estratégicos:

   - Identificar casos de lavado sofisticado
   - Fortalecer el trabajo conjunto entre procesos, identificando diferentes fuentes de información que puedan proyectar casos operacionales
   - Analizar la totalidad de la información reportada en UIAF

b. **Estrategia 2. Prevención:** aumentar la efectividad en la prevención del lavado de activos y la financiación del terrorismo, para que los actores del Sistema ALA-CFT adopten mecanismos, instrumentos y medidas, que además de ajustarse a las 40 Recomendaciones de GAFI y los atributos definidos por la Unidad, se logre obtener información de calidad para el Sistema Dinámico y Efectivo, con el fin de proteger la economía nacional y contribuir con el bienestar de los colombianos.

Objetivos Estratégicos:

- Fortalecer la coordinación entre los actores responsables para dinamizar el Sistema ALA-CFT
- Establecer mecanismos de aprendizaje para los actores del Sistema ALA-CFT
- Originar un mayor grado de conocimiento técnico en los diferentes actores del Sistema ALA-CFT

c. **Estrategia 3. Detección:** fortalecer el trabajo conjunto con la FGN y adelantar actividades coordinadas con homólogos u organismos internacionales de similar naturaleza, donde se aborden temas LA/FT de gran impacto para detectar economías ilícitas, las cuales deberán ser investigadas y juzgadas por las autoridades competentes en relación con el lavado de activos los delitos fuente (Art 323 Código Penal).
Objetivos Estratégicos:

- Establecer metodologías de análisis para mesas de trabajo y working groups buscando impacto
- Priorizar la contestación de requerimientos que conducen a la detección de casos de impacto

d. **Estrategia 4. Transformación tecnológica e innovación:** implementar proyectos de trasformación tecnológica que soporten el desarrollo del Sistema dinámico y efectivo de la Unidad, apalancándose en herramientas innovadoras como machine Learning, procesamiento de redes complejas, modelos matemáticos computacionales, ingeniería de software y flujos de trabajo, para optimiza y potencializar los procesos misionales del ciclo de inteligencia determinados por la entidad, y así se entreguen información oportuna para la toma de decisiones.

Objetivos Estratégicos:

- Adoptar tecnología (hardware, software y procesos) que agilice y simplifique los procesos de análisis de información
- Centralizar las diferentes entradas de información y atender las necesidades de la áreas y demás instancias

e. **Estrategia 5. Seguimiento intensificado: articulación + cooperación:** desarrollar acciones encaminadas a incrementar las recalificaciones de las Recomendaciones de GAFILAT, con el fin de que mediante el uso óptimo de la plataforma Egmont, se puedan identificar oportunidad para el desmantelamiento de las redes criminales de carácter transnacional, que mediante el contrabando, el narcotráfico, la minería ilegal, la corrupción, la trata de personas, el terrorismo, y otros fenómenos criminales, utilizan los canales y las vías del comercio internacional para ocultar el origen ilícito o darles apariencia de legalidad de los bienes obtenidos mediante estas actividades.

Objetivos Estratégicos:

- Utilizar y optimizar la plataforma Egmont para la efectiva detección y el desmantelamiento de las redes criminales de carácter transnacional
- Superar las deficiencias identificadas por el IEM de GAFILAT de 2018, mediante las solicitudes de recalificaciones de las Recomendaciones 13, 16 y 33 ante el GAFILAT y hacer seguimiento a los compromisos internacionales asumidos por la UIAF

f. **Estrategia 6. Política Ruta de la Felicidad: capital humano + conocimiento:** implementar la Política Ruta de la Felicidad con el fin aumentar el compromiso permanente y la efectividad de los servidores para la creación de valor público, su desarrollo profesional y personal en el cumplimiento de las estrategias planeadas y así orientarse hacia una transformación de la cultura organizacional.

Objetivos Estratégicos:

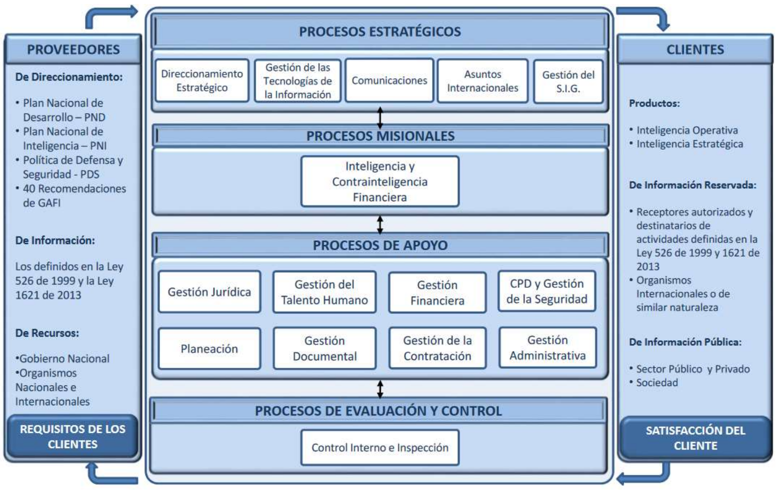
- Realizar seguimiento a la implementación de la Política Ruta de la Felicidad y sus planes correspondientes
- Crear estrategias comunicacionales con el fin de que todos los servidores incorporen la política y los beneficios de la misma
- Aplicar mecanismos que permitan evaluar la productividad de los servidores
- Aplicar mecanismos que permitan evaluar la felicidad de los servidores, a partir de los resultados iniciales del 2020

g. **Estrategia 7. Gestión de la administración:** hacer uso de la cultura de "hacer bien las cosas" donde se refleje la calidad y la integridad de toda la Unidad, con el fin de posicionar a la UIAF como un modelo moderno de gestión pública.

Objetivos Estratégicos:

- Fortalecer el funcionamiento general del sistema de gestión SIG
- Mejorar la calificación del modelo MIPG y en general los indicadores e índices de la gestión pública
- Liderar los proyectos de restructuración de planta y adecuación de instalaciones

7.5. Mapa de Procesos:

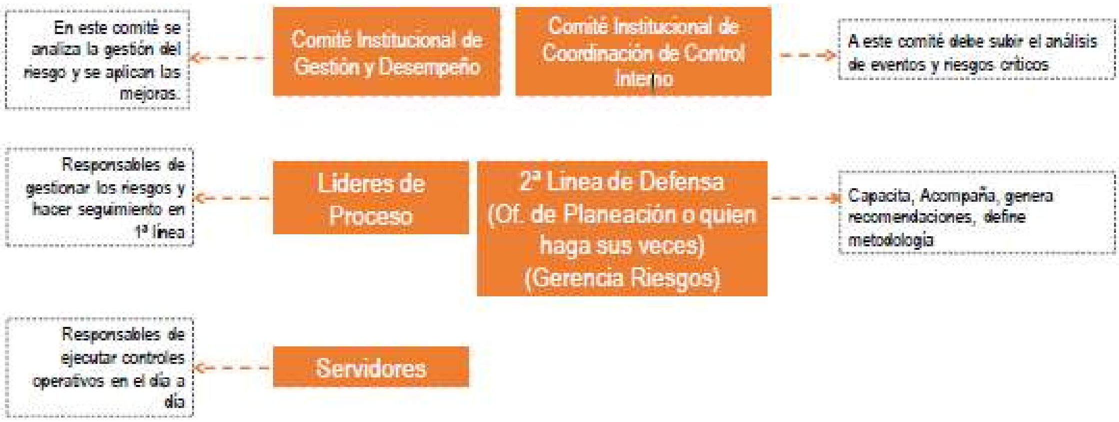


8. METODOLOGÍA

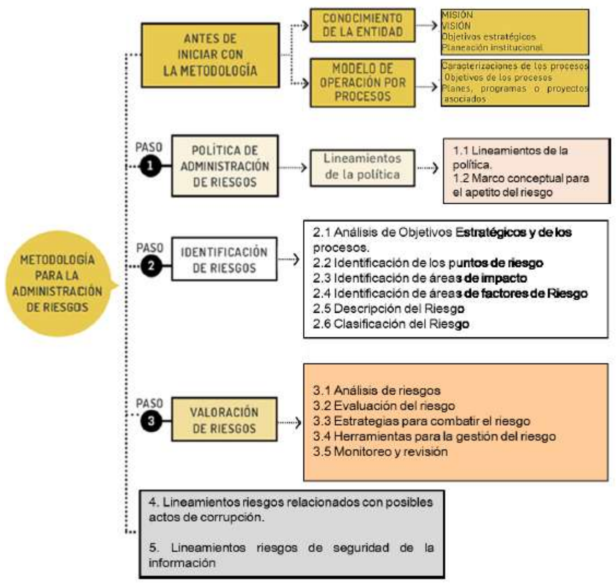
La Unidad de Información y Análisis Financiero – UIAF adopta la metodología establecida por el Departamento Administrativo de la Función Pública – DAFP, a través de la Guía para la administración del riesgo y diseño de controles en entidades públicas, versión 5, diciembre de 2020.

De igual manera, se incorporan los lineamientos definidos en el Modelo Integrado de Planeación y Gestión – MIPG, la Guía para la identificación y declaración del conflicto de intereses en el Sector Público colombiano, emitida por el Departamento Administrativo de la Función Pública – DAFP.

De otra parte, el Modelo Integrado de Planeación y Gestión (MIPG) define para su para su operación articulada la creación en todas las entidades del Comité Institucional de Gestión y Desempeño, regulado por el Decreto 1499 de 2017 y el Comité Institucional de Coordinación de Control Interno, reglamentado a través del artículo 13 de la Ley 87 de 1993 y el Decreto 648 de 2017, en este marco general, para una adecuada gestión del riesgo, dicha institucionalidad entra a funcionar de la siguiente forma:



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 ésta 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, tal como se muestra a continuación:



8.1. Establecimiento del contexto de la entidad

Antes de iniciar con la metodología para la administración de los riesgos, es necesario comprender el entorno y analizar el contexto general de la entidad (factores internos y externos), para establecer el Marco Estratégico para los próximos cuatro años. Este Marco Estratégico, parte de un análisis de contexto que permite conocer en dónde se encuentra la entidad y cuál será su direccionamiento para el siguiente periodo de gobierno.

El contexto general de la entidad está conformado por el **contexto externo** (**factores:** políticos, económicos, financieros, sociales, culturales, tecnológicos, ambientales, legales y reglamentarios); **el contexto interno** (**factores:** estructura organizacional, funciones y responsabilidades, estratégicos, el recurso humano, los procesos, la tecnología, la información, la comunicación interna); **contexto del proceso** (**factores:** diseño, interrelación con otros procesos, transversalidad, procedimientos, planes, programas, proyectos, activos de información).

Categoría del Contexto	Factores
Externo	**Políticos:** cambios de gobierno, legislación, políticas públicas, regulación.
	Económicos y financieros: disponibilidad de capital, liquidez, mercados financieros, desempleo, competencia.
	Sociales y culturales: demografía, responsabilidad social, orden público.
	Tecnológicos: avances en tecnología, acceso a sistemas de información externos, gobierno digital.
	Ambientales: emisiones y residuos, energía, catástrofes naturales, desarrollo sostenible.
	Legales y reglamentarios: normatividad externa (leyes, decretos, ordenanzas y acuerdos)
Interno	**Financieros:** presupuesto de funcionamiento e inversión, infraestructura.
	Personal: competencia del personal, disponibilidad del personal, seguridad y salud en el trabajo, trabajo en equipo y liderazgo.
	Procesos: capacidad, diseño, ejecución, proveedores, entradas, salidas, gestión del conocimiento.
	Tecnología: integridad de datos, disponibilidad de datos y sistemas, desarrollo, producción
	Estratégicos: planeación estratégica.
	Comunicación interna: canales utilizados y su efectividad, flujo de la información necesaria para el desarrollo de las operaciones.
Proceso	**Diseño del proceso:** claridad en la descripción del alcance y objetivo del proceso.
	Interacciones con otros procesos: relación precisa con otros procesos en cuanto a insumos, proveedores, productos, usuarios y clientes.
	Transversalidad: procesos que determinan lineamientos necesarios para el desarrollo de todos los procesos de la entidad.
	Procedimientos asociados: pertinencia en los procedimientos que desarrollan los procesos.
	Responsables del proceso: grado de autoridad y responsabilidad de los funcionarios frente al proceso.
	Comunicación entre los procesos: efectividad en los flujos de información determinados en la interacción de los procesos.
	Activos de seguridad digital del proceso: información, aplicaciones, hardware entre otros, que se debe proteger para garantizar el funcionamiento interno de cada proceso, como de cara al ciudadano.

Seguridad de la información:

Con el fin de profundizar en el análisis relacionado con seguridad digital, se deben considerar los siguientes factores relacionados con el entorno digital:

Factores Externos	Factores Internos	Factores de los Procesos
Clientes, proveedores de servicios y empresas que sean competencia directa y/o se relacionen con la misión de la entidad pública analizada.	Recursos económicos, sociales, ambientales, físicos, tecnológicos, financieros, jurídicos, entre otros.	Identificación de los procesos y su respectiva caracterización.
Normativas o aspectos jurídicos que apliquen directa o indirectamente a la entidad pública; ejemplo, la ley 1581 de 2012 o la ley 1712 de 2014, circulares o regulaciones emitidas por superintendencias o ministerios, como el decreto 1078 de 2015 o el decreto 1499 de 2017.	Flujos de información y los procesos de toma de decisiones.	Detalle de las actividades que se llevan a cabo en el proceso.
Dependencias económicas y financieras por parte de otras empresas.	Objetivos estratégicos y la forma de alcanzarlos.	Detalle de las actividades que se llevan a cabo en el proceso.
Entorno cultural	Empleados, contratistas.	Flujos de información.
Cualquier otro factor externo de tipo internacional, nacional (gobierno), regional o local.	La misión, visión, valores y cultura de la organización.	Identificación y actualización de los activos en la cadena de valor de la entidad pública.
Cantidad de ciudadanos a los cuales la entidad pública brinda servicios a través del entorno digital como trámites a través de páginas web.	Sus políticas, procesos y procedimientos.	Recursos.
Aspectos externos que pueden verse afectados con los riesgos de seguridad digital, tales como el ambiente social, económico y ambiental que tengan alguna relación con las operaciones asociadas a la entidad pública.	Sistemas de gestión (calidad, seguridad en el trabajo, seguridad de la información, riesgos, entre otros).	Relaciones con otros procesos de la entidad pública.
	Toda la estructura organizacional.	Alcance del proceso.
	Roles y responsabilidades.	Cantidad de ciudadanos afectados por el proceso.
	Sistemas de información o servicios.	Procesos de gestión de riesgos que se tienen actualmente implementados.
		Personal involucrado en la toma de decisiones.

Para llevar a cabo esta actividad, se sugiere hacer una lista en la que estén enumeradas las partes interesadas externas e internas que tengan relación con la entidad y con sus objetivos, misión o visión.

8.2. Identificación del Riesgo:

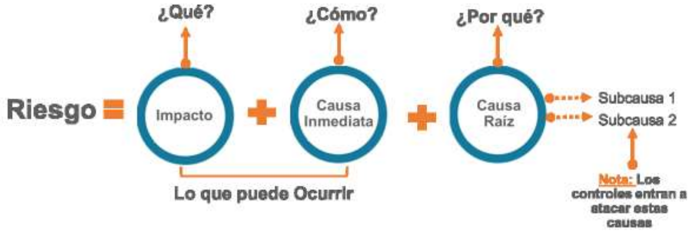
El conocimiento del contexto estratégico facilita la identificación de los riesgos y las oportunidades para el cumplimiento de los objetivos estratégicos, dado que permite establecer cuáles son los riesgos asociados a la operación de la entidad y determinar cuáles están identificados, controlados y cuáles no.

La identificación del riesgo, se realiza a través de las siguientes fases:

- **Análisis de los 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.
- **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.
- **Identificación de áreas de impacto:** el área de impacto es la consecuencia económica o reputacional a la cual se ve expuesta la entidad en caso de materializarse un riesgo. Los impactos que aplican son afectación económica (o presupuestal) y reputacional.
- **Identificación de áreas de factores de riesgo:** son las fuentes generadoras de riesgos. Algunos factores de riesgo que puede tener una entidad son:

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

- **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:



Esta 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.

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

Premisas para una adecuada redacción del riesgo:

- No describir como riesgos omisiones ni desviaciones del control.
  Ejemplo: errores en la liquidación de la nómina por fallas en los procedimientos existentes.

- No describir causas como riesgos
  Ejemplo: inadecuado funcionamiento de la plataforma estratégica donde se realiza el seguimiento a la planeación.

- No describir riesgos como la negación de un control
  Ejemplo: retrasos en la prestación del servicio por no contar con digiturno para la atención.

- No existen riesgos transversales, lo que pueden existir son causas transversales.
  Ejemplo: pérdida de expedientes.

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

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

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

Categoría	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.

Identificación de los riesgos de corrupción:

Definición de 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. "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).

La entidad debe seleccionar los procesos, procedimientos o actividades que considere que son susceptibles de actos de corrupción, sobre los cuales pueda adelantar el análisis del contexto interno, para la correspondiente identificación de los riesgos de corrupción, entre los cuales se pueden analizar los siguientes:

Proceso, Procedimiento o Actividad	Factores de Riesgos
Direccionamiento Estratégico (alta dirección)	• Concentración de autoridad o exceso de poder. • Extralimitación de funciones. • Ausencia de canales de comunicación. • Amiguismo y clientelismo
Financiero (está relacionado las áreas de planeación y presupuesto)	• Inclusión de gastos no autorizados. • Inversiones de dineros públicos en entidades de dudosa solidez financiera a cambio de beneficios indebidos para servidores públicos encargados de su administración. • Inexistencia de registros auxiliares que permitan identificar y controlar los rubros de inversión. • Inexistencia de archivos contables. • Afectar rubros que no corresponden con el objeto del gasto en beneficio propio o a cambio de una retribución económica.
Contratación	• Estudios previos o de factibilidad deficientes.

Proceso, Procedimiento o Actividad	Factores de Riesgos
(como proceso o bien los procedimientos ligados a este)	• Estudios previos o de factibilidad manipulados por personal interesado en el futuro proceso de contratación. (Estableciendo necesidades inexistentes o aspectos que benefician a una firma en particular). • Pliegos de condiciones hechos a la medida de una firma en particular. • Disposiciones establecidas en los pliegos de condiciones que permiten a los participantes direccionar los procesos hacia un grupo en particular. (Ej.: media geométrica). • Visitas obligatorias establecidas en el pliego de condiciones que restringen la participación. • Adendas que cambian condiciones generales del proceso para favorecer a grupos determinados. • Urgencia manifiesta inexistente. • Concentrar las labores de supervisión en poco personal. • Contratar con compañías de papel que no cuentan con experiencia.
Información y Documentación	• Ausencia o debilidad de medidas y/o políticas de conflictos de interés. • Concentración de información de determinadas actividades o procesos en una persona. • Ausencia de sistemas de información que pueden facilitar el acceso a información y su posible manipulación o adulteración. • Ocultar la información considerada pública para los usuarios. • Ausencia o debilidad de canales de comunicación.
Investigación y Sanción	• Inexistencia de canales de denuncia interna o externa. • Dilatar el proceso para lograr el vencimiento de términos o la prescripción de este. • Desconocimiento de la ley mediante interpretaciones subjetivas de las normas vigentes para evitar o postergar su aplicación. • Exceder las facultades legales en los fallos.
Trámites y/o Servicios internos y externos	• Cobros asociados al trámite. • Influencia de tramitadores. • Tráfico de influencias: (amiguismo, persona influyente).
Reconocimiento de un Derecho (expedición de licencias y/o permisos)	• Falta de procedimientos claros para el trámite. • Imposibilitar el otorgamiento de una licencia o permiso. • Tráfico de influencias: (amiguismo, persona influyente).

Para la identificación de riesgos de corrupción, la entidad también puede utilizar fuentes de datos externas como organismos de control o vigilancia o información del sector al cual pertenece y que permitan identificar situaciones irregulares que pueden llegar a ser comunes en las entidades públicas, que sirvan de referente para realizar el análisis propio de la entidad.

A nivel interno, se pueden realizar entrevistas con el personal, revisión de las denuncias interpuestas a través de los diferentes canales que se encuentren implementados, así como la evaluación de incentivos, las presiones, la potencial eliminación de controles por parte de la dirección, el análisis de las áreas donde los controles son débiles o no existe una adecuada segregación de funciones.

Otro factor interno es la tecnología, por lo que se deben considerar los accesos a los sistemas, las amenazas internas y externas a la integridad de los datos, la seguridad de los sistemas y el posible robo de información confidencial o sensible.

Las preguntas clave para la identificación del riesgo son:

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

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 utiliza la matriz de definición de riesgo de corrupción porque incorpora cada uno de los componentes de su definición.

Si en la descripción del riesgo, las casillas son contestadas todas afirmativamente, se trata de un riesgo de corrupción, así:

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

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 + BENEFICIO PRIVADO

Identificación de los riesgos de seguridad digital:

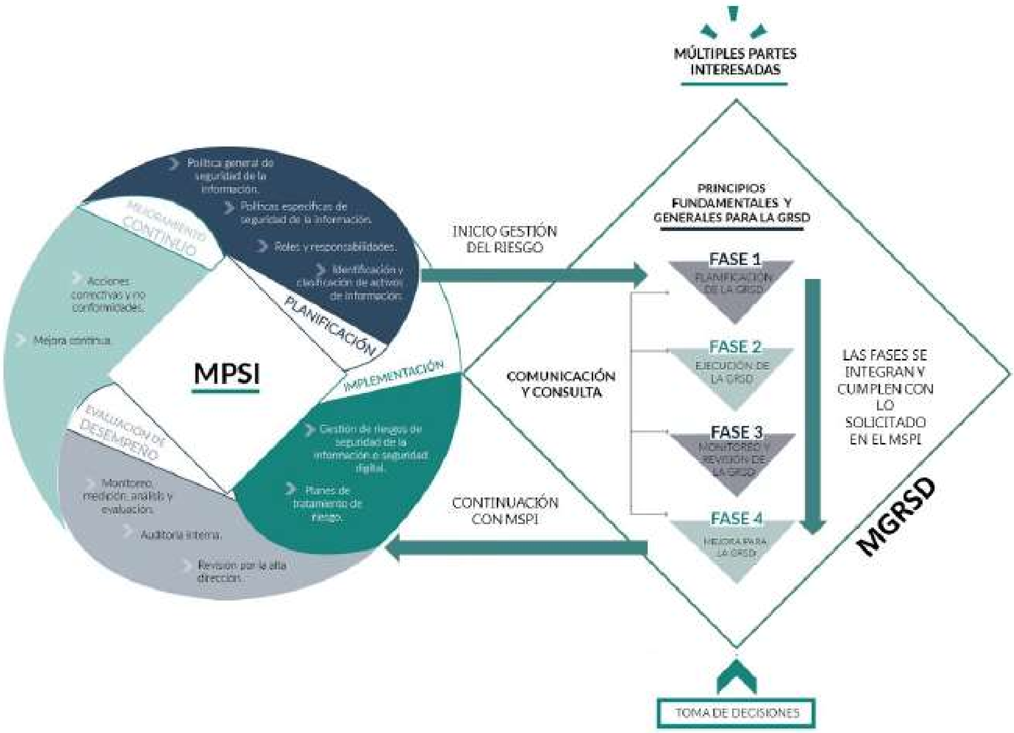
Se debe tener en cuenta que la Política de Seguridad Digital se vincula al Modelo de Seguridad y Privacidad de la Información (MSPI), el cual se encuentra alineado con el Marco de Referencia de Arquitectura TI y soporta transversalmente los otros habilitadores de la política de gobierno digital: Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales.

En esencia, la interacción entre ambos modelos puede resumirse de la siguiente manera:

- Las actividades de identificación de activos, identificación, análisis, evaluación y tratamiento de los riesgos se alinean con la fase de PLANIFICACIÓN del MSPI.
- Las actividades de implementación de los planes de tratamiento de riesgos se alinean con la fase de IMPLEMENTACIÓN del MSPI.

- Las actividades de monitoreo y revisión, revisión de los riesgos residuales, efectividad de los planes de tratamiento o los controles implementados y auditorías se alinean con la fase de MEDICIÓN DEL DESEMPEÑO del MSPI.
- Las actividades de MEJORAMIENTO CONTINUO en ambos modelos son similares y trabajan simultáneamente, ya que dependerán de las fases de Medición del Desempeño para identificar aspectos a mejorar en la aplicación de ambos Modelos.

Interacción entre el Modelo de Seguridad y Privacidad de la Información – MSPI y el Modelo de Gestión del Riesgo de Seguridad Digital – MGRSD:



Como primer paso para la identificación de los riesgos de seguridad de la información, es necesario identificar los activos de información de cada proceso. Estos permiten determinar qué es lo más importante que la entidad y sus procesos posee (bases de datos, archivos, servidores web o aplicaciones clave para que la entidad pueda prestar sus servicios). 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.

Identificación de activos de seguridad digital:

Definición de activo: es cualquier elemento que tenga valor para la organización, sin embargo, en el contexto de seguridad digital, son activos elementos tales como: aplicaciones informáticas de la entidad, servicios web, redes, información física o digital, tecnologías de la información TI, tecnologías de operación TO que utiliza la entidad para funcionar en el entorno digital.

Es necesario que la entidad identifique los activos y documente un inventario de activos, así podrá saber lo que se debe proteger para garantizar tanto su funcionamiento interno (BackOffice) como su funcionamiento de cara al ciudadano (FrontOffice), aumentando así su confianza en el uso del entorno digital para interactuar con el Estado.

La identificación y valoración de activos debe ser realizada por la Primera Línea de Defensa – Líderes de Proceso, en cada proceso donde aplique la gestión del riesgo de seguridad digital, siendo debidamente orientados por el responsable de seguridad digital o de seguridad de la información de la entidad.

Pasos para la identificación y valoración de activos:

Corresponde al líder del Sistema de Gestión de Seguridad y Privacidad de la Información y al líder del proceso o proyecto la identificación de los riesgos de la Información. Estos se basan en la afectación de tres criterios en un activo de información o un grupo de activos de información dentro del proceso: "Integridad, confidencialidad o disponibilidad".

Al realizar la identificación del contexto externo, la entidad debería tener plenamente identificados los aspectos regulatorios y normativos con los que deberá cumplir, las leyes enunciadas (1712 de 2014 y 1581 de 2012) pueden ser de cumplimiento para la mayoría de las entidades públicas, sin embargo, es tarea de la misma entidad determinar si hay más o menos aspectos regulatorios a tener en cuenta respecto a la información. El área jurídica de la entidad debe colaborar en esta tarea específica.

Para identificar los activos, realizar su inventario y clasificación, la entidad puede emplear los siguientes métodos:

- Revisión de los flujos o diagramas del proceso.
- Revisión de inventarios de activos previos o de otras áreas.
- Entrevistas o lluvia de ideas dentro de cada proceso.
- Reuniones con expertos que tienen el mayor conocimiento del tema.
- Realizar análisis de escenarios.

La **Guía para la gestión y clasificación de activos del Modelo de Seguridad y Privacidad de la Información** de la Estrategia Gobierno Digital de MINTIC, capítulo 7, también brinda una orientación para clasificar los activos de información.

La entidad puede decidir si realiza la gestión de riesgos en todos los activos identificados o si desea hacerlo a los activos más críticos. Esta decisión debe estar debidamente formalizada en el procedimiento de gestión de activos que solicita el Modelo de Seguridad y Privacidad de la Información. Adicionalmente, debe quedar explícita en la Política de Administración de Riesgos de la entidad, debidamente aprobada por el Comité Institucional de Coordinación de Control Interno.

Identificación del riesgo inherente de seguridad digital:

De acuerdo con lo indicado en la "Guía para la Administración del Riesgo en la Gestión, Corrupción y Seguridad Digital. Diseño de Controles en Entidades Públicas", 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 debe 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 de amenazas comunes:

Tipo	Amenaza	Origen
Daño físico	Fuego	F, D, A
	Agua	F, D, A
Eventos naturales	Fenómenos climáticos	E
	Fenómenos sísmicos	E
Pérdidas de los servicios esenciales	Fallas en el sistema de suministro de agua	E
	Fallas en el suministro de aire acondicionado	F, D, A
Perturbación debida a la radiación	Radiación electromagnética	F, D, A
	Radiación térmica	F, D, A
Compromiso de la información	Interceptación de servicios de señales de interferencia comprometida	D
	Espionaje remoto	D
Fallas técnicas	Fallas del equipo	D, F
	Mal funcionamiento del equipo	D, F
	Saturación del sistema de información	D, F
	Mal funcionamiento del software	D, F
	Incumplimiento en el mantenimiento del sistema de información	D, F
Acciones no autorizadas	Uso no autorizado del equipo	D, F
	Copia fraudulenta del software	D, F
Compromiso de las funciones	Error en el uso o abuso de derechos	D, F
	Falsificación de derechos	D

Tabla de amenazas dirigidas por el hombre:

Fuente de amenaza	Motivación	Acciones amenazantes
Pirata informático, intruso ilegal	Reto Ego	Piratería
		Ingeniería Social
Criminal de la computación	Destrucción de la información	Crimen por computador

Fuente de amenaza	Motivación	Acciones amenazantes
	Divulgación ilegal de la información	Acto fraudulento
Terrorismo	Chantaje Destrucción	Ataques contra el sistema
		DDoS
		Penetración en el sistema
Espionaje industrial (inteligencia, empresas, gobiernos extranjeros, otros intereses)	Ventaja competitiva Espionaje económico	Ventaja de defensa
		Hurto de información
Intrusos (empleados con entrenamiento deficiente, descontentos, malintencionados, negligentes, deshonestos o despedidos)	Curiosidad Ganancia monetaria	Asalto a un empleado
		Chantaje

Tabla de vulnerabilidades comunes:

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

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

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.

8.3. Valoración del riesgo:

Consiste en establecer la probabilidad de ocurrencia del riesgo y el nivel de consecuencia o impacto, con el fin de estimar la zona de riesgo inicial (Riesgo Inherente).

a. **Análisis de riesgos:** busca establecer la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto, con el fin de estimar la zona de riesgo inicial (Riesgo Inherente). La probabilidad de ocurrencia está 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.

Bajo este esquema, la subjetividad que usualmente afecta este tipo de análisis se elimina, ya que se puede determinar con claridad la frecuencia con la que se lleva a cabo una actividad, en vez de considerar los posibles eventos que pudiesen haberse dado en el pasado, ya que bajo esta óptica, si nunca se han presentado eventos, todos los riesgos tendrán la tendencia a quedar ubicados en niveles bajos, situación que no es real frente a la gestión de las entidades públicas colombianas.

Determinación de la probabilidad de ocurrencia en riesgos de gestión: e analiza a partir de la pregunta ¿qué tan posible es que ocurra el riesgo? Está asociada a la exposición al riesgo del proceso o actividad que se está analizando, puede tratarse de un hecho que no se ha presentado pero es posible que se presente, es decir, al número de veces que se pasa por el punto de riesgo en el periodo de 1 año, o tratándose de hechos que se han materializado o frente a los cuales se cuenta con un historial de situaciones o eventos asociados al riesgo.

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%

Determinación de la probabilidad en riesgos de corrupción: la determinación de la probabilidad (posibilidad de ocurrencia del riesgo) se debe llevar a cabo bajo los mismos criterios establecidos para los riegos de gestión. La frecuencia se relaciona con la ejecución de la actividad de la cual proviene el riesgo de corrupción. Es decir, se debe considerar desde el objetivo del proceso y su exposición al riesgo, en este sentido, tomando la misma tabla para realizar el análisis.

Determinación de la probabilidad en riesgos de seguridad digital: la determinación de la probabilidad (posibilidad de ocurrencia del riesgo) se debe llevar a cabo bajo los mismos criterios establecidos para los riegos de gestión. La frecuencia se relaciona con la ejecución de la actividad de la cual proviene el riesgo de seguridad digital. Es decir, se debe considerar desde el objetivo del proceso y su exposición al riesgo, en este sentido, tomando la misma tabla para realizar el análisis.

Determinación del impacto o consecuencia en riesgos de gestión: permite establecer las consecuencias o efectos del riesgo, con el fin de estimar la zona de riesgo en caso de no controlarse (Riesgo Inherente). Para definir la tabla de criterios, las variables principales que se tienen en cuenta son impactos económicos y reputacionales.

De presentarse el impacto económico y reputacional en un solo riesgo con diferentes niveles, se debe tomar el nivel más alto, lo que facilita el análisis para el líder del proceso, dado que se puede considerar información objetiva para su establecimiento, eliminando la subjetividad que usualmente puede darse en este tipo de análisis.

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

Determinación del impacto en riesgos de corrupción: para la determinación del impacto frente a posibles materializaciones de riesgos de corrupción, se analizarán únicamente los siguientes niveles i) moderado, ii) mayor, y iii) catastrófico, dado que estos riesgos siempre serán significativos, en tal sentido, no aplican los niveles de impacto leve y menor, que sí aplican para las demás tipologías de riesgos.

Criterios para calificar el impacto en riesgos de corrupción:

N.º	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. Nivel de impacto MAYOR	10	
MODERADO	Genera medianas consecuencias sobre la entidad		
MAYOR	Genera altas consecuencias sobre la entidad.		

Determinación del impacto en riesgos de seguridad digital: la determinación del impacto se debe llevar a cabo de acuerdo con lo establecido en el aparte 3.1.2 de la "Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 5", bajo los mismos criterios establecidos para los riegos de gestión, entendiendo que el impacto se entiende como la consecuencia económica y reputacional que se genera por la materialización del riesgo.

El nivel de impacto en los riesgos de seguridad digital, deberá ser determinado con la presencia de cualquiera de los criterios establecidos, tomando el criterio con mayor valor de afectación, ya sea cualitativo o cuantitativo.

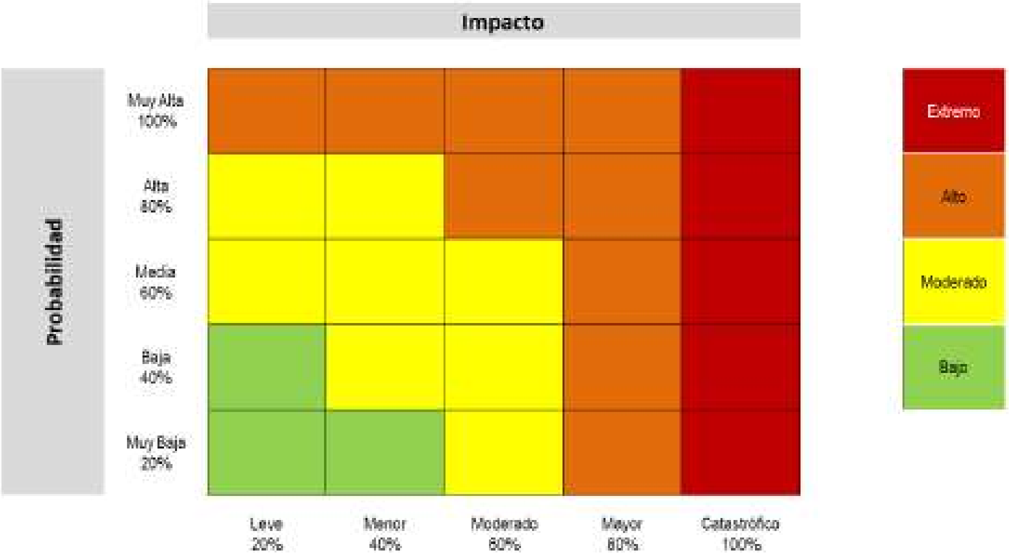
La probabilidad y el impacto se determinan con base a la amenaza y no en las vulnerabilidades.

Determinación del impacto de pérdida de continuidad de negocio: la determinación de las prioridades de recuperación de servicios en caso de materialización de escenarios de pérdida de continuidad de negocio, se realiza mediante la valoración del impacto percibido por los líderes de los procesos, para lo cual se programan mesas de trabajo, en las que los participantes califican los impactos en cada variable y definen el orden de recuperación de los servicios, asignando la secuencia de reactivación de los mismos primero a los servicios con mayor impacto y de manera secuencial a los servicios con menor impacto percibido.

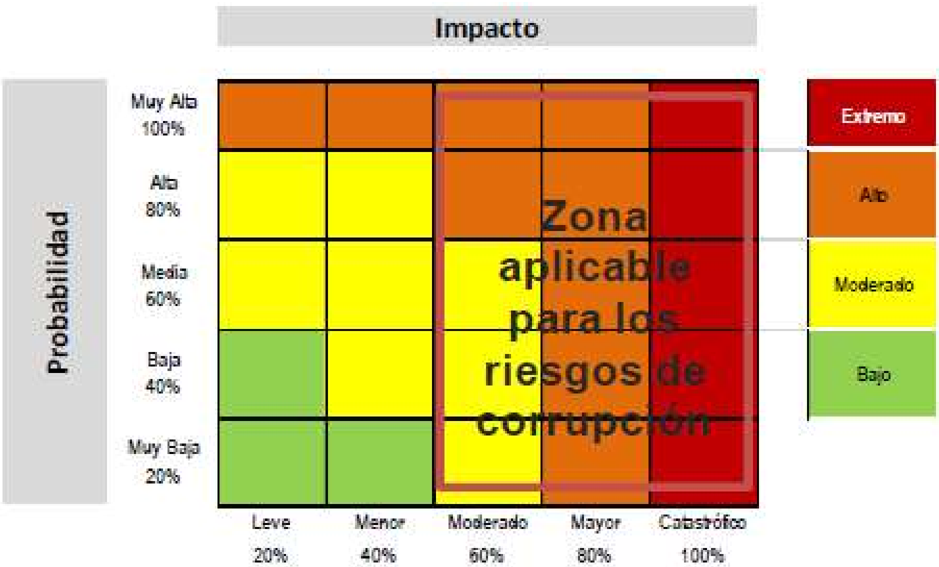
b. Evaluación de riesgos: se busca confrontar los resultados del análisis de riesgo inicial frente a los controles establecidos, con el fin de determinar la zona de riesgo final (Riesgo residual).

A partir del análisis de la probabilidad de ocurrencia del riesgo y sus consecuencias o impactos, se busca determinar la zona de riesgo inicial (Riesgo Inherente).

Valoración del riesgo de gestión. En la etapa de análisis preliminar (riesgo inherente), se trata de determinar los niveles de severidad a través de la combinación entre la probabilidad y el impacto, a través de la definición de 4 zonas de severidad en la matriz de calor, así:



Valoración del riesgo de corrupción. En la etapa de análisis preliminar (riesgo inherente), se define el nivel de severidad para el riesgo de corrupción identificado, para lo cual se aplica la matriz de calor establecida en el numeral 3.2.1 de la Guía para la administración del riesgo y el diseño de controles en entidades pública – versión 5, teniendo en cuenta el ajuste frente a los niveles de impacto leve y menor mencionados en la determinación del impacto, lo que implica que las zonas de severidad para este tipo de riesgos se delimita como se muestra a continuación:



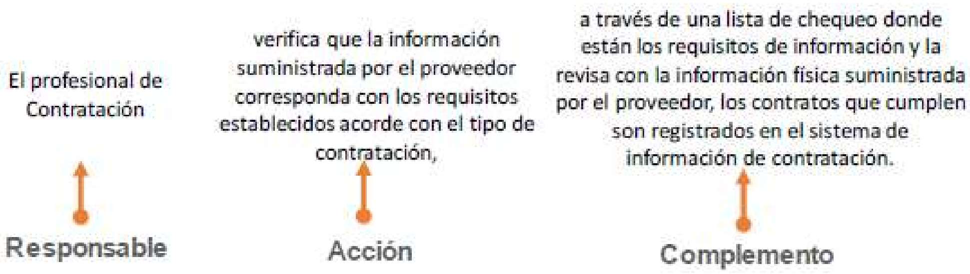
Valoración del riesgo de seguridad digital. Para el análisis preliminar (riesgo inherente), se define el nivel de severidad para el riesgo de seguridad de la información identificado, mediante la aplicación de la misma matriz de calor establecida para determinar la severidad para los riesgos de gestión.

Valoración de controles en riesgos de gestión: conceptualmente un control se define como la medida que permite reducir o mitigar el riesgo, para lo cual 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.

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.



Tipología de controles y los procesos: a través del ciclo de los procesos se establece cuándo se activa un control y, por lo tanto, establecer su tipología con mayor precisión. Para comprender esta estructura conceptual, en la siguiente figura se consideran 3 fases globales del ciclo de un proceso así:

De acuerdo con la anterior figura, 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.

De acuerdo con la forma como se ejecutan los controles tenemos:

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

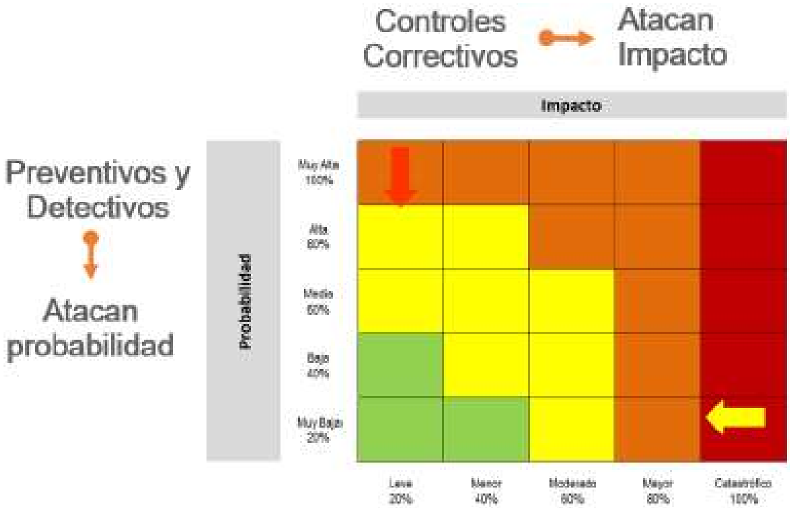
Análisis y evaluación de los controles – atributos: a continuación se analizan los atributos para el diseño del control, teniendo en cuenta características relacionadas con la eficiencia y la formalización, la descripción y el peso asociados a cada uno:

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	25%

Características			Descripción	Peso
			intervención de personas para su realización.	
		Manual	Controles que son ejecutados por una persona, tiene implícito el error humano.	15%
*Atributos informativos	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	El control se aplica siempre que se realiza la actividad que conlleva el riesgo.	-
		Aleatoria	El control se aplica aleatoriamente a la actividad que conlleva el riesgo	-
	Evidencia	Con registro	El control deja un registro permite evidencia la ejecución del control.	-
		Sin registro	El control no deja registro de la ejecución del control.	-

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 siguiente 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:



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 estos mitigan el riesgo de forma acumulativa, es 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.

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.

Valoración de controles en riesgos de corrupción: se aplicarán las disposiciones establecidas en el numeral 3.2.2 y en el capítulo 3 de la "Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 5", para la valoración de los controles en la gestión de riesgos de corrupción.

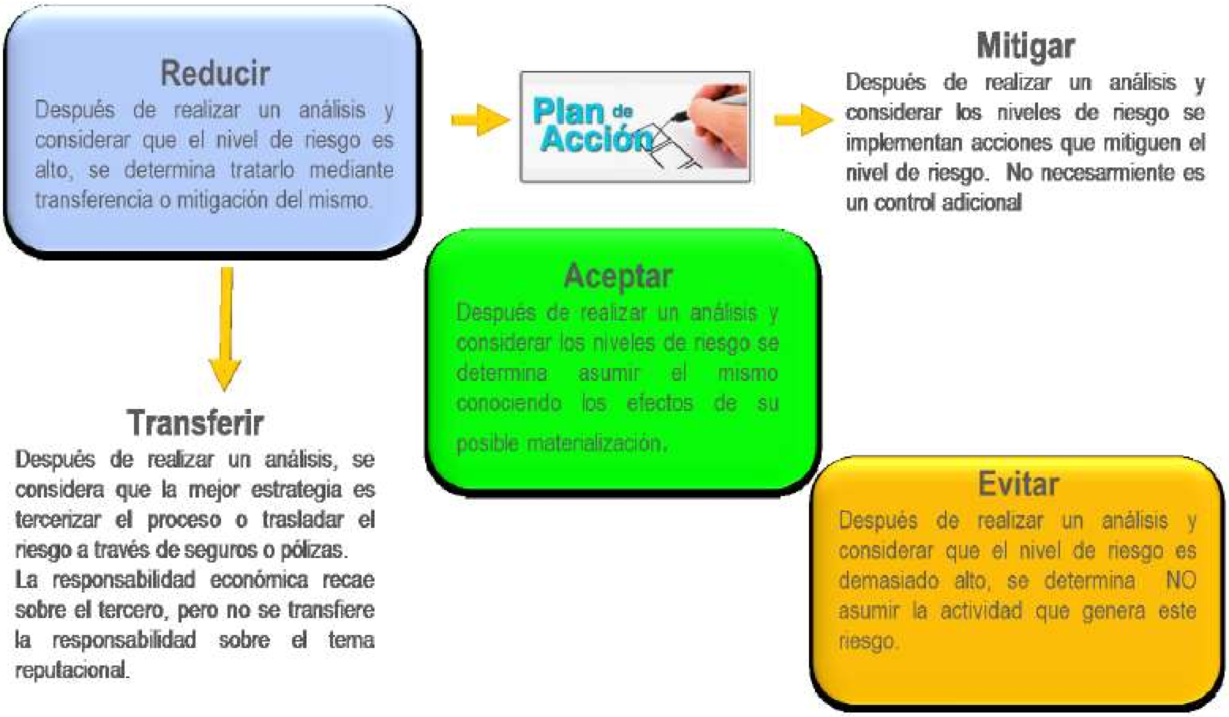
Valoración de controles en riesgos de seguridad digital: la entidad podrá mitigar/tratar los riesgos de seguridad de la información empleando como mínimo los controles del Anexo A de la norma técnica ISO/IEC 27001:2013, estos controles se encuentran en el anexo 4. "Modelo Nacional de Gestión de riesgo 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.

8.4. 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 para procesos en funcionamiento, cuando se trate de procesos nuevos, se procede a partir del riesgo inherente.

Frente al plan de acción referido para la opción de reducir, es importante mencionar que, conceptualmente y de manera general, se trata de una herramienta de planificación empleada para la gestión y control de tareas o proyectos.

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. Este plan de acción, es diferente al plan de contingencia, el cual se enmarca dentro del Plan de Continuidad de Negocio y sería considerado un control correctivo.



A partir de los criterios Reducir, Aceptar y Evitar, se establecen las siguientes acciones para los niveles de aceptación a los riesgos así:

Criterio	Acciones
Aceptar	Se debe asumir el riesgo y el impacto de su materialización en caso que se presente.
Evitar	Se debe eliminar, evitar o cambiar la actividad generadora del riesgo.
Reducir	Adoptar acciones para abordar riesgos encaminadas a reducir, mitigar o transferir el riesgo, no necesariamente las acciones es un control adicional.

8.5. Monitoreo y revisión:

El Modelo Integrado de Planeación y Gestión (MIPG) desarrolla a través de la dimensión 7 - Control Interno las líneas de defensa para identificar la responsabilidad de la gestión del riesgo y control que está distribuida en los diversos servidores de la entidad.

Como mínimo, anualmente los líderes de proceso con el apoyo y acompañamiento de Planeación y de la Oficina de Control Interno, identifican y/o validan los riesgos de gestión, de corrupción y de seguridad digital asociados al logro de los objetivos de los procesos y objetivos institucionales.

El monitoreo y revisión de los riesgos se realizará en primera instancia por el responsable del proceso y en instancias posteriores por las auditorías internas programadas por la Oficina de Control Interno.

El monitoreo a los riesgos de gestión, riesgos de corrupción y seguridad digital deberá realizarse cuatrimestralmente, con corte a abril 30, a agosto 31 y a diciembre 31. Este monitoreo debe incluir la actualización de los riesgos y los respectivos mapas de riesgos, si se presentan cambios en el proceso que genere nuevos riesgos o se requiera modificar los factores determinantes que modifiquen la valoración de los riesgos identificados.

Monitoreo y revisión a los riesgos de seguridad digital:

A través de las Tres Líneas de Defensa definidas en la Dimensión 7 - Control Interno, Componente Actividades de Control del Modelo Integrado de Planeación y Gestión - MIPG, la entidad debe hacer un seguimiento a los planes de tratamiento para determinar su efectividad, de acuerdo con lo definido a continuación:

- Realizar seguimiento y monitoreo al plan de acción en la etapa de implementación y finalización de los planes de acción.
- Revisar periódicamente las actividades de control para determinar su relevancia y actualizarlas de ser necesario.
- Realizar monitoreo de los riesgos y controles tecnológicos.
- Efectuar la evaluación del plan de acción y realizar nuevamente la valoración de los riesgos de seguridad digital para verificar su efectividad.
- Verificar que los controles están diseñados e implementados de manera efectiva y operen como se pretende para controlar los riesgos.
- Suministrar recomendaciones para mejorar la eficiencia y eficacia de los controles.

Una vez que el plan de tratamiento de riesgos se haya ejecutado en las fechas y con las disposiciones de recursos previstas, la entidad debe valorar nuevamente el riesgo y verificar si el nivel disminuyó o no (es decir, si se desplazó de una zona mayor a una menor en el mapa de calor) y luego, compararlo con el último nivel de riesgo residual.

En esta fase se deben evaluar periódicamente los riesgos residuales para determinar la efectividad de los planes de tratamiento de riesgos y de los controles propuestos, de acuerdo con lo definido en la Política de Administración de Riesgos de la entidad. Así mismo, también deberá tenerse en cuenta los incidentes de seguridad digital que hayan afectado a la entidad y también las métricas o indicadores definidos para hacer seguimiento a las medidas de seguridad implementadas. Todo lo anterior contribuye a la toma de decisiones en el proceso de revisión de riesgo por parte de la línea estratégica (Alta dirección y Comité Institucional de Coordinación de Control Interno) y las partes interesadas.

Registro y reporte de incidentes de seguridad digital: es importante que la entidad cuente con el registro de los incidentes de seguridad digital que se hayan materializado, con el fin de analizar las causas, las deficiencias de los controles implementados y las pérdidas que se pueden generar.

El propósito fundamental del registro de incidentes es garantizar que se tomen las acciones adecuadas para evitar o disminuir su ocurrencia, retroalimentar y fortalecer la identificación y gestión de dichos riesgos y enriquecer las estadísticas sobre amenazas y vulnerabilidades y, con esta información, adoptar nuevos controles.

Reporte de la gestión del riesgo de seguridad digital al interior de la entidad: el responsable de seguridad digital deberá reportar periódicamente a la Línea Estratégica (Alta dirección y Comité Institucional de Coordinación de Control Interno) y a las partes interesadas la siguiente información:

- Matriz de los riesgos de seguridad digital identificados.
- Listado de activos críticos TI/TO y listado de la Infraestructura Crítica Cibernética.
- Reporte de criticidad / impacto de la entidad.
- Plan de Tratamiento de Riesgos.
- Reporte de evolución de riesgos y modificación del apetito del riesgo.
- Cantidad de riesgos por fuera de la tolerancia del riesgo identificados de acuerdo con la periodicidad de evaluación realizada.
- Impacto económico que podría presentarse frente a la materialización de los riesgos.

Auditorías internas y externas: le corresponde a la **Oficina de Control Interno (tercera línea de defensa)**, realizar evaluación (aseguramiento) independiente sobre la gestión del riesgo de seguridad digital en la entidad, catalogándola como una unidad auditable más dentro de su Universo de Auditoría, conforme al Plan Anual de Auditoría aprobado por el Comité Institucional de Coordinación de Control Interno de la entidad.

9. NIVELES DE ACEPTACIÓN DEL RIESGO

Los niveles de aceptación del riesgo se determinan como resultado de la valoración de la probabilidad de ocurrencia del riesgo y de la magnitud del impacto al momento de evaluar su materialización. Los riesgos de gestión inherentes ubicados en la zona de riesgos baja pueden ser aceptados y por lo tanto no es necesario establecer controles. Los riesgos de corrupción son los únicos que son inaceptables en todo sentido, por tanto, deben tener controles permanentes de seguimiento.

9.1. Niveles de aceptación para pos riesgos de gestión

a. **Zona de Riesgo Baja:** Se **ASUMIRÁ** el riesgo y se administra por medio de las actividades propias del proyecto o proceso asociado y se realiza en el reporte TRIMESTRAL de su desempeño.
b. **Zona de Riesgo Moderada:** Se establecen acciones de control preventivas que permitan reducir la probabilidad de ocurrencia del riesgo y se hace seguimiento **TRIMESTRAL**.
c. **Zona de Riesgo Alta y Zona de Riesgo Extrema:** Se incluyen estos riesgos en el Mapa de Riesgos Institucional, se establecen acciones de control preventivas que permitan **MITIGAR** la materialización del riesgo y se monitorean **MENSUALMENTE**.

9.2. Niveles de aceptación para los riesgos de corrupción

a. **Zona de Riesgo Baja:** Ningún riesgo de corrupción podrá ser aceptado. Se Realizarán seguimientos **MENSUALES** por parte de los líderes de los procesos para evitar a toda costa su materialización.
b. **Zona de Riesgo Moderada:** Se establecen acciones de control preventivas que permitan **REDUCIR** la probabilidad de ocurrencia del riesgo. Se realizarán seguimientos MENSUALES por parte de los líderes de los procesos, para evitar a toda costa su materialización.
c. **Zona de Riesgo Alta y Zona de Riesgo Extrema:** Se adoptan medidas para: **REDUCIR** la probabilidad o el impacto del riesgo o ambos; por lo general conlleva a la implementación de controles; **EVITAR**, se

abandonan las actividades que dan lugar al riesgo, decidiendo no iniciar o no continuar con la actividad que causa el riesgo; **TRANSFERIR O COMPARTIR** una parte del riesgo para reducir la probabilidad o el impacto del mismo. Se realizan seguimientos **MENSUALES** por parte de los líderes de los procesos, para evitar a toda costa su materialización.

10. HISTORIA DE CAMBIOS DEL DOCUMENTO

Versión	Motivo del Cambio	Descripción del Cambio	Fecha del Cambio
1	Versión inicial	Elaboración del documento de política	11 de Enero de 2017
2	Revisión y actualización de la Política de Administración del Riesgo	Revisión de la Política de Administración de Riesgos, respecto a los cambios normativos establecidos en el Decreto 648 de 2017 y en la Guía para la administración del riesgo del y el diseño de controles en entidades públicas. Riesgos de gestión, corrupción y seguridad digital. Versión 4. Octubre de 2018.	19 de Diciembre de 2018
3	Revisión y actualización con base en la nueva guía metodológica emitida por el DAFP.	Se actualiza la Política de Administración del riesgo de acuerdo con los lineamientos establecidos por el Departamento Administrativo de la Función Pública – DAFP, a través de la "Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 5, diciembre de 2020".	22 de Diciembre de 2021