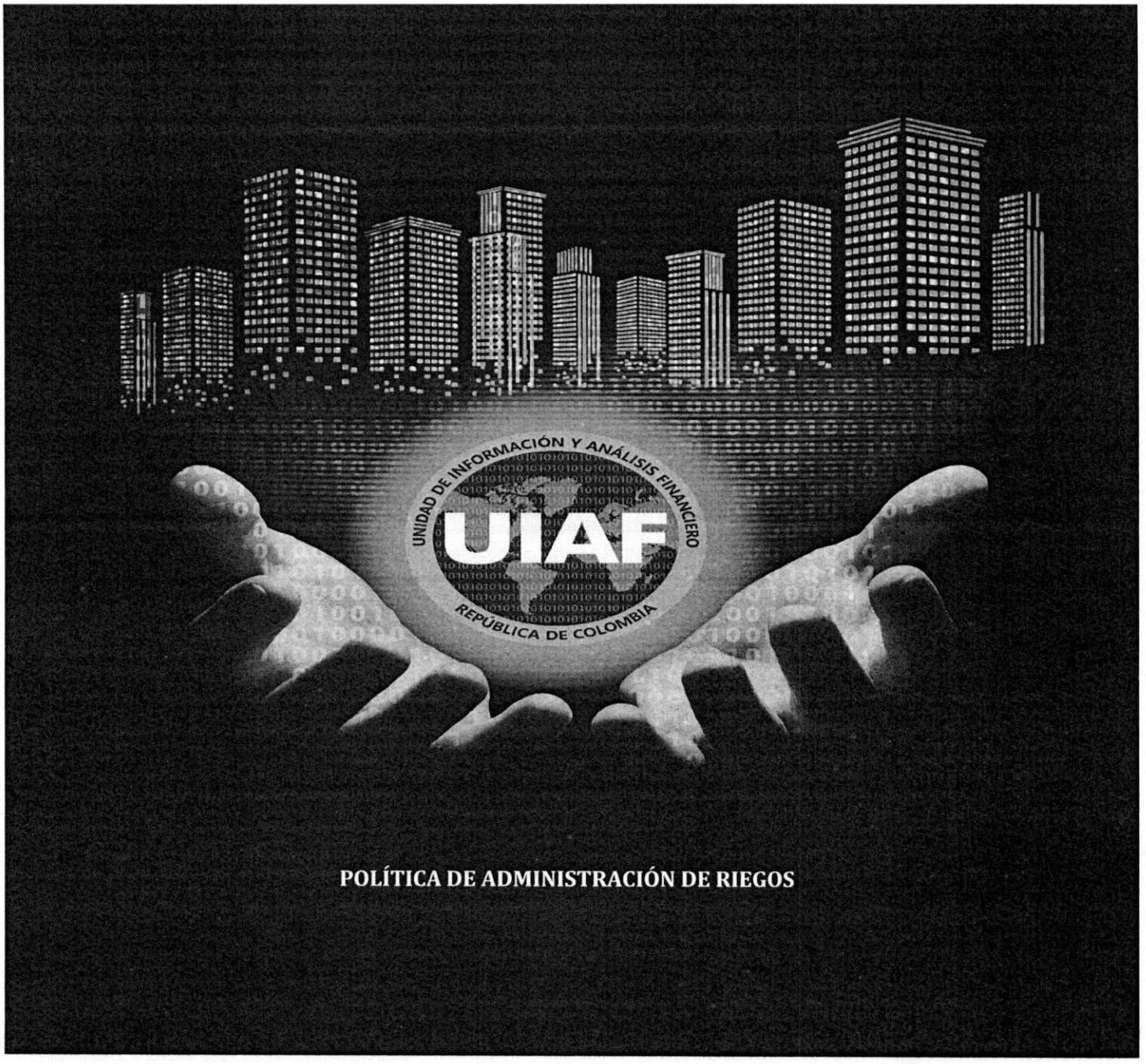


POLÍTICA DE ADMINISTRACIÓN DE RIEGOS

	PREPARÓ	REVISÓ	APROBÓ
FIRMA:			
CÓDIGO:	302	320, 241, 342, 355, 321, 108, 313, 21, 88, 310, 165,352, 296	108
CARGO:	Profesional Especializado OAP	Subdirectora SAO, Subdirector SAE, Subdirector de SAN, Subdirector STI, Subdirectora SAF, Jefe OAJ, Jefe OAI, Jefe OCII, Profesional Especializado OCII, Jefe OAP (E), Profesional Especializado OAP, Profesional Especializado OAP, Profesional Universitario OAP	Director General (E)
FECHA:	24 de agosto 2023	05 de junio de 2024	05 de junio de 2024

Tabla de Contenido

Lista de Tablas

Lista de Ilustraciones

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 y Contrainteligencia Financiera, a fin de detectar y prevenir el lavado de activos, la financiación del terrorismo, financiamiento a la proliferación de armas de destrucción masiva, delitos ambientales, operaciones sospechosas en los sectores financiero y real de la economía, tanto interna como externa, que pueda tener relación directa o indirecta con actividades de contrabando y fraude aduanero (Leyes 526 de 1999, 1121 de 2006 y 1762 de 2015).

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

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, están siempre expuestas a diferentes riesgos o eventos que pueden poner en peligro su existencia.

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 forma positiva o negativa el logro de sus objetivos institucionales. Así mismo, se pretende transmitir el enfoque de la Alta Dirección sobre la manera de abordarlos; socializar con los funcionarios un lenguaje común, y difundir la política formulada que permita la sostenibilidad del sistema de manejo de riesgos. Además, contribuye a que la entidad consolide su Sistema de Control Interno y se genere una cultura de Autocontrol y Autoevaluación en el interior de la misma, de acuerdo con lo establecido en el Modelo Integrado de Planeación y Gestión– MIPG y en particular, la Política de Control Interno.

1. OBJETIVO

Establecer los lineamientos y criterios que orienten la identificación, valoración, tratamiento, monitoreo y seguimiento a los riesgos.

2. ALCANCE

Aplicable a todos los planes, programas, proyectos y procesos del modelo de operación de la entidad.

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;
- Ley 87 de 1993 "Por medio del cual se establecen normas para el ejercicio de control interno en las entidades y organismos del Estado y se dictan otras disposiciones";

- Ley 489 de 1998, "Por medio del cual se fortalece el Control Interno, mediante la creación del Sistema Nacional de Control Interno";
- Ley 526 de 1999" Por medio del cual se crea la Unidad de Información y Análisis Financiero"; Reglamentada parcialmente por Decreto 1497 del 2002 y modificada por la Ley 1121 del 29 de diciembre de 2006;
- Ley 610 de 2000 "Por medio del cual se establece el trámite de los procesos de responsabilidad fiscal de competencia de las contralorías";
- Ley 1121 de 2006 "Por medio del cual se dictan normas para la prevención, detección, investigación y sanción de la financiación del terrorismo y otras disposiciones";
- Ley 1437 de 2011" Por medio del cual se expide el Código de Procedimiento Administrativo y de lo Contencioso Administrativo";
- Ley 1581 de 2012 "Por medio del cual se dictan disposiciones generales para la protección de datos personales"; Reglamentada parcialmente por el Decreto Nacional 1377 de 2013, y por el Decreto 1081 de 2015;
- Ley 1562 de 2012" Por medio del cual se modifica el sistema de riesgos laborales y se dictan otras disposiciones en materia de salud ocupacional";
- Ley 1621 de 2013" Por medio del cual se expiden normas para fortalecer el marco jurídico que permite a los organismos que llevan a cabo actividades de inteligencia y contrainteligencia cumplir con su misión constitucional y legal, y se dictan otras disposiciones";
- Ley 1712 de 2014 "Por medio del cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública y Nacional y se dictan otras disposiciones";
- Ley 1952 de 2019 "Por medio del cual se expide el código general disciplinario se derogan la ley 734 de 2002 y algunas disposiciones de la ley 1474 de 2011, relacionadas con el derecho disciplinario." Artículo 44. Conflicto de intereses;
- Decreto Nacional 1377 de 2013" Por medio del cual se reglamenta parcialmente la Ley 1581 de 2012 y se dictan disposiciones generales para la protección de datos personales";
- Decreto 857 de 2014, Por medio del cual se reglamenta la Ley Estatutaria 1621 del 17 de abril de 2013," Por medio de la cual se expiden normas para fortalecer el marco legal que permite a los organismos, que llevan a cabo actividades de inteligencia y contrainteligencia, cumplir con su misión constitucional y legal y se dictan otras disposiciones";
- Decreto 1083 de 2015, última fecha de actualización 15 de junio de 2023" Por medio del cual se expide el Decreto único reglamentario del sector de Función Pública";
- Decreto 1078 de 2015 "Por medio del cual se expide el Decreto Único Reglamentario del sector de tecnologías de la información y las comunicaciones";
- Decreto 1076 de 2015 "Por medio del cual se expide el Decreto Único Reglamentario del Sector Ambiente y Desarrollo Sostenible";
- Decreto 1072 de 2015 "Por medio del cual se dictan disposiciones para la implementación del Sistema de Gestión de la Seguridad y Salud en el Trabajo (SG-SST)";
- Decreto 648 de 2017 "Por medio del cual se modifica y adiciona el Decreto 1083 de 2015, Reglamentario Único del Sector de la Función Pública en cuanto al régimen de ingreso, administración de personal, situaciones administrativas, retiro de los empleados públicos";
- Decreto 1499 de 2017 "Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015";
- Decreto 612 de 2018 "Por medio del cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado";

- Decreto 1008 de 2018 "Por medio del 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";
- Decreto 403 de 2020 "Por el cual se dictan normas para la correcta implementación del Acto Legislativo 04 de 2019 y el fortalecimiento del control fiscal";
- Decreto 153 de 2022 "Por medio del cual se modifica la planta de personal de la Unidad de Información y Análisis Financiero (UIAF)";
- Decreto 152 de 2022 "Por medio del cual se modifica la estructura de la Unidad de Información y Análisis Financiero (UIAF)";
- Decreto 1497 de 2002 "Por medio del cual se reglamenta parcialmente la Ley 526 de 1999 y se dictan otras disposiciones";
- Resolución 76 de 2022" Por medio del cual se actualiza la conformación 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, acorde con el Decreto No. 152 de 28 de enero de 2022";
- Resolución 127 de 2022" Por medio del cual se modifica el Mapa de Procesos de la Unidad de Información y Análisis Financiero – UIAF";
- Resolución 128 de 2022" Por medio del cual se integra y se establece el reglamento de funcionamiento del Comité Institucional de Gestión y Desempeño de la Unidad de Información y Análisis Financiero – UIAF";
- Resolución 129 de 2022" Por medio del cual se conforma y adopta el Sistema Integrado de Gestión de la Unidad de Información y Análisis Financiero – UIAF";
- Resolución 33 de 2023 "Por medio del cual se adopta el Plan Estratégico Institucional – 2023-2026"
- Guía para la identificación de los peligros y la valoración de los riesgos en Seguridad y Salud Ocupacional GTC 45:2012;
- Acto legislativo 04 de 2019, Por medio del cual se reforma el Régimen de Control Fiscal;
- Gestión del riesgo ambiental principios y procesos – GTC 104 -2009;
- Guía para la administración del riesgo y el diseño de controles en entidades públicas - versión 6 de 2022;
- Modelo Integrado de Planeación y Gestión – MIPG – versión 5 de 2023.

4. TÉRMINOS Y DEFINICIONES

- **Alta Dirección:** persona o grupo de personas del máximo nivel jerárquico que dirigen y controlan una entidad (ISO 9000 versión 2015).
- **Accidente de Trabajo:** es todo suceso repentino que sobrevenga por causa o con ocasión del trabajo, y que produzca en el trabajador una lesión orgánica, una perturbación funcional o psiquiátrica, una invalidez o la muerte (Artículo 3 de la Ley 1562 de 2012).
- **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 (Manual Metodología de Riesgos versión 7 de 2022).
- **Administración de Riesgos**: actividades coordinadas para dirigir y controlar la organización con relación a los riesgos (Norma NTC-ISO 31000:2018).
- **Amenaza:** Situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización (Manual Metodología de Riesgos versión 7 de 2022).
- **Análisis de Riesgo:** el propósito del análisis de riesgos es comprender la naturaleza de los riesgos y sus características incluyendo, cuando sea apropiado, el nivel de los riesgos mismos (Norma NTC-ISO 31000:2018).
- **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 (Manual Metodología de Riesgos versión 7 de 2022).

- **Auditoría:** proceso sistemático, independiente y documentado para obtener evidencias objetivas y evaluarlas de manera objetiva con el fin de determinar el grado en que se cumplen los criterios de auditoría (Norma NTC- ISO 19011:2018).
- **Auditoría Conjunta:** auditoría llevada a cabo a un único auditado por dos o más organizaciones auditoras. (Norma NTC- ISO 19011:2018).
- **Autorización:** consentimiento previo, expreso e informado del titular para llevar a cabo el tratamiento de datos personales (Ley estatutaria 1581 de 2012).
- **Base de Datos:** conjunto organizado de datos personales que sea objeto de tratamiento (Ley estatutaria 1581 de 2012).
- **Bien Público**: son todos aquellos muebles e inmuebles de propiedad pública. Estos se clasifican en bienes de uso público y bienes fiscales (Guía para la administración del Riesgo y el diseño de controles en entidades públicas – versión 6).
  - **Bienes de uso público:** aquellos cuyo uso pertenece a todos los habitantes del territorio nacional (ejemplo: las calles, plazas, puentes, vías parques, etc.).
  - **Bienes Fiscales:** aquellos que están destinados al cumplimiento de las funciones públicas o servicios públicos, es decir afectos al desarrollo de su misión y utilizados para sus actividades.
- **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 (Guía para la administración del Riesgo y el diseño de controles en entidades públicas – versión 6).
- **Causa:** todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo (Guía para la administración del Riesgo y el diseño de controles en entidades públicas – versión 6).
- **Causa Inmediata:** circunstancias bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo (Guía para la administración del Riesgo y el diseño de controles en entidades públicas – versión 6).
- **Causa Raíz:** causa principal o básica, corresponde a las razones por la cuales se puede presentar el riesgo (Guía para la administración del Riesgo y el diseño de controles en entidades públicas – versión 6).
- **Circunstancias Inmediatas:** se trata de aquella situación o actividad bajo la cual se presenta el riesgo, pero no constituyen la causa principal o básica- causa raíz (Guía para la administración del Riesgo y el diseño de controles en entidades públicas – versión 6).
- **Compartir el Riesgo:** cuando es muy difícil para la entidad reducir el riesgo a un nivel aceptable o se carece de conocimientos necesarios para gestionarlo, este puede ser compartido con otra parte interesada que pueda gestionarlo con más eficacia. Cabe señalar que normalmente no es posible transferir la responsabilidad del riesgo (Guía para la administración del Riesgo y el diseño de controles en entidades públicas – versión 6).
- **Competencia:** atributos personales y aptitud demostrada para aplicar conocimientos y habilidades (Guía GTC 45:2012).
- **Confidencialidad:** propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados (Guía para la administración del Riesgo y el diseño de controles en entidades públicas – versión 6).
- **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 "Todo servidor público deberá declararse impedido para actuar en un asunto cuando tenga interés particular y directo en su regulación, gestión, control o decisión, o lo tuviere su cónyuge, compañero o

compañera permanente, o algunos de sus parientes dentro del cuarto grado de consanguinidad, segundo de afinidad o primero civil, o su socio o socios de hecho o de derecho."

- **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 (Guía para la administración del Riesgo y el diseño de controles en entidades públicas – versión 6).
- **Contingencia:** posibilidad de que algo suceda o no suceda (RAE)
- **Control:** Medida que permite reducir o mitigar un riesgo (Guía para la administración del Riesgo y el diseño de controles en entidades públicas – versión 6).
- **Criterios de Auditoria:** conjunto de requisitos usados como referencia frente a la cual se compara la evidencia objetiva (NTC ISO 19011: 2018).
- **Datos Personales:** por la cual se dictan disposiciones generales para la protección de datos personales. (Ley Estatuaria 1581 de 2012).
- **Disponibilidad:** propiedad de ser accesible y utilizable a demanda por una entidad (Guía para la administración del Riesgo y el diseño de controles en entidades públicas - versión 6).
- **Eficacia:** grado en el que se realizan las actividades planificadas y se logran los resultados planificados. (NTC ISO 19011: 2018).
- **Encargado del Tratamiento:** persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el tratamiento de datos personales por cuenta del responsable del tratamiento (Ley Estatutaria 1581 de 2012).
- **Evaluación del Riesgo:** su propósito es identificar, evaluar y gestionar eventos potenciales, tanto internos como externos, que puedan afectar el logro de los objetivos institucionales. (Guía para la administración del Riesgo y el diseño de controles en entidades públicas - versión 6).
- **Evidencia de la Auditoria:** registros, declaraciones de hechos o cualquier otra información que es pertinente para los criterios de auditoría y que es verificable (NTC ISO 19011: 2018).
- **Factores de Riesgo:** son las fuentes generadoras de riesgos (Guía para la Administración del Riesgo y el diseño de controles en entidades públicas - versión 6).
- **Gestión del Riesgo Fiscal**: son las actividades que debe desarrollar cada Entidad y todos los gestores públicos (ver concepto de gestor público) para identificar, valorar, prevenir y mitigar los riesgos fiscales (probabilidad de efecto dañoso sobre los bienes, recursos y/o intereses patrimoniales de naturaleza pública, a causa de un evento potencial), (Guía para la Administración del Riesgo y el diseño de controles en entidades públicas - versión 6).
- **Gestor Fiscal:** son los servidores públicos y las personas de derecho privado que manejen o administren recursos o fondos públicos, desarrollando actividades económicas, jurídicas y tecnológicas, tendientes a la adecuada y correcta adquisición, planeación, conservación, administración, custodia, explotación, enajenación, consumo, adjudicación, gasto, inversión y disposición de los bienes (Guía para la Administración del Riesgo y el diseño de controles en entidades públicas - versión 6).
- **Gestor Público:** es todo aquel que participa, concurre, incide o contribuye directa o indirectamente en el manejo o administración de bienes, recursos o intereses patrimoniales de naturaleza pública, sean o no gestores fiscales, por lo tanto, son todos los gestores públicos y no sólo los que desarrollan gestión fiscal, los llamados a prevenir riesgos fiscales (Guía para la Administración del Riesgo y el diseño de controles en entidades públicas - versión 6).
- **Identificación del peligro:** proceso para reconocer si existe un peligro (véase el numeral 2.27) y definir sus características. (GTC 45:2012).
- **Impacto:** las consecuencias que puede ocasionar a la organización la materialización del riesgo. (Guía para la Administración del Riesgo y el diseño de controles en entidades públicas - versión 6).
- **Incidente:** evento(s) relacionado(s) con el trabajo, en el (los) que ocurrió o pudo haber ocurrido lesión o enfermedad (independiente de su severidad) o víctima mortal (GTC 45:2012).

- **Integridad:** propiedad de exactitud y completitud (Guía para la Administración del riesgo y el diseño de controles en entidades públicas - versión 6).
- **Patrimonio Público:** se entiende como el conjunto de bienes o recursos o intereses patrimoniales de naturaleza pública, susceptibles de estimación económica (Guía para la Administración del riesgo y el diseño de controles en entidades públicas - versión 6).
- **Punto de Riesgo:** actividades en las que potencialmente se genera riesgo. (Guía para la Administración del riesgo y el diseño de controles en entidades públicas - versión 6).
- **Plan de Auditoría:** descripción de las actividades y de los detalles acordados de una auditoría (NTC ISO 19011:2018)
- **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. (Guía para la administración del Riesgo y el diseño de controles en entidades públicas – versión 6)
- **Mapa de Riesgo:** documento que resume los resultados de las actividades de gestión de riesgos, incluye una representación gráfica en modo de mapa de calor de los resultados de la evaluación de riesgos.
- **Nivel de Consecuencia (NC):** medida de la severidad de las consecuencias (GTC 45:2012).
- **Nivel de Deficiencia (ND):** magnitud de la relación esperable entre (1) el conjunto de peligros detectados y su relación causal directa con posibles incidentes y (2) con la eficacia de las medidas preventivas existentes en un lugar de trabajo. (GTC 45:2012)
- **Nivel de Exposición (NE):** situación de exposición a un peligro que se presenta en un tiempo determinado durante la jornada laboral. (GTC 45:2012).
- **Nivel de Probabilidad (NP):** producto del nivel de deficiencia (GTC 45:2012).
- **Nivel de Riesgo:** Magnitud de un riesgo resultante del producto del nivel de probabilidad por el nivel de consecuencia (GTC 45:2012).
- **Política:** intenciones y dirección de una organización como las expresa formalmente su alta dirección (ISO 9000:2015).
- **Probabilidad:** se entiende la posibilidad de ocurrencia del riesgo. (Guía para la Administración del riesgo y el diseño de controles en entidades públicas - versión 6).
- **Proceso:** conjunto de actividades mutuamente relacionadas que utilizan las entradas para proporcionar un resultado previsto (ISO 9000:2015).
- **Programa de Auditoría:** conjunto de una o más auditorías planificadas para un periodo de tiempo determinado y dirigidas hacia un propósito específico (ISO 9000:2015).
- **Recurso Público:** para efectos del capítulo de riesgos fiscales, entiéndase como recurso público, los dineros comprometidos y ejecutados en ejercicio de la función pública. (Guía para la Administración del riesgo y el diseño de controles en entidades públicas - versión 6).
- **Requisito:** necesidad o expectativa establecida, generalmente implícita u obligatoria (ISO 9000:2015).
- **Riesgo:** efecto de la incertidumbre (ISO 19011:2018).
- **Riesgo Aceptable:** riesgo que ha sido reducido a un nivel que la organización puede tolerar con respecto a sus obligaciones legales y su propia política en seguridad y salud ocupacional (GTC 45:2012/NTC-OHSAS 18001)
- **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 (Guía para la administración del riesgo y el diseño de controles en entidades públicas - versión 6).
- **Riesgo de Continuidad en el Negocio:** es la probabilidad de que ocurra una afectación en los procesos que pueden comprometer la disponibilidad de funciones de negocio.
- **Riesgos de Datos Personales:** información personal que ha sido registrada, procesada y no ha sido salvaguarda en una entidad.

- **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 de Seguridad Digital:** es la expresión usada para describir una categoría de riesgo relacionada con el desarrollo de cualquier actividad en el entorno digital. Este riesgo puede resultar de la combinación de amenazas y vulnerabilidades en el ambiente digital (Tomado de la política nacional de seguridad digital).
- **Riesgo en Seguridad y Salud en el Trabajo:** combinación de la probabilidad de que ocurra una o más exposiciones o eventos peligrosos y la severidad del daño que puede ser causada por estos.
- **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 6).
- **Riesgo Fiscal:** es el efecto dañoso sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública, a causa de un evento potencial (Tomado de la guía para la administración del riesgo y el diseño de controles en entidades públicas - versión 6).
- **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 6).
- **Sistema de Gestión:** conjunto de elementos de una organización interrelacionados o que interactúan para establecer políticas, objetivos y procesos para lograr estos objetivos (ISO 45001:2018)
- **Tolerancia del Riesgo:** es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del Apetito de riesgo determinado por la entidad (Guía para la Administración del Riesgo y el diseño de controles en entidades públicas - versión 6).
- **Valoración de los Riesgos:** proceso de evaluar el(los) riesgo(s) que surge(n) de un(os) peligro(s), teniendo en cuenta la suficiencia de los controles existentes, y de decidir si el(los) riesgo(s) es (son) aceptable(s) o no (GTC 45:2012).
- **Vulnerabilidad:** representan la debilidad de un activo o de un control que puede ser explotada por una o más amenazas (Guía para la Administración del Riesgo y el diseño de controles en entidades públicas - versión 6 de 2022).

5. ROLES Y RESPONSABILIDADES FRENTE AL RIESGO

Para asegurar las responsabilidades en la gestión del riesgo, se asigna los roles 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 6 de 2022.

Tabla 1. Roles y responsabilidades

Línea Estratégica Define el marco general para la gestión del riesgo y el control y supervisa su cumplimiento, está a cargo de la Alta Dirección y el Comité Institucional de Coordinación de Control Interno.	
a. Roles y Responsabilidades	**Responsables**
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.	**Alta Dirección** (Equipo Directivo) **Comité Institucional de Coordinación de Control Interno** (Resolución 76 de 31 de marzo de 2022) (Director General, Subdirectores, Jefes de Oficina) **Comité Institucional de Gestión y Desempeño** (Resolución 128 de mayo 24 de 2022) (Director General, Subdirectores, Jefes de Oficina)
b. Actividades a Realizar	
1. Fortalecer el Comité Institucional de Coordinación de Control Interno, incrementando su periodicidad para las reuniones; 2. Definir y aprobar 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 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	
1. 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.	

Primera Línea de Defensa Desarrolla e implementa procesos de control y gestión de riesgos a través de su identificación, análisis, valoración, monitoreo y acciones de mejora	
a. Roles y Responsabilidades	**Responsables**
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.	**Líderes de Procesos, Programas y Proyectos** Dirección General, Subdirecciones, oficinas asesoras y grupo de comunicaciones.
b. Actividades a Realizar	

1. Revisar los cambios en el direccionamiento estratégico o en el entorno y cómo estos pueden generar nuevos riesgos o modificar los existentes en cada uno de los procesos; 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 vigente y establecida por el Departamento Administrativo de la Función Pública -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 planes 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.	
c. Comunicación y Consulta	
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.	
d. Accionar ante la Materialización del Riesgo	
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 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.	

2da. Línea de Defensa Asegurar que los controles y procesos de gestión del riesgo de la primera línea sean aprobados y funcionen correctamente	
a. Roles y Responsabilidades	**Responsables**
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.	**Jefe de planeación o quien haga sus veces**
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 digital, 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 o 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 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.	

Tercera Línea de Defensa Proporciona información sobre la 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	
a. Roles y Responsabilidades	**Responsables**
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; 3. Recomendar mejoras a las políticas de operación para la administración del riesgo.	**Oficina de Control Interno o quien haga sus veces**
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; 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.

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas. Versión 6 y 5. Marco General del Modelo Integrado de Planeación y Gestión. Versión 5

5.1. Roles y Responsabilidades de Continuidad del Negocio

Funciones y responsabilidades que se asignan a los diversos responsables que hacen parte de la Gestión de Continuidad del Negocio en la Unidad de Información y Análisis Financiero. Para cada rol identificado, se definieron sus respectivas responsabilidades como se muestra a continuación:

Tabla 2. Roles y responsabilidades de continuidad del negocio

Comité Institucional de Gestión y Desempeño	
Funciones en la respuesta y recuperación	Asumir la toma de decisiones estratégicas ante las comunicaciones, medios y responsables: 1. Minimizar el impacto en la UIAF ante una crisis que pueda afectar la imagen reputacional, operatividad a largo plazo, responsabilidades legales, comunicaciones y los medios de comunicación; 2. Asegurarse que las prioridades se entienden claramente y el flujo de información en las comunicaciones son adecuados a las exigencias de la situación de acuerdo con un Plan de Gestión de Crisis; 3. Asistir y participar activamente de las pruebas, capacitaciones y divulgación definidas por el responsable de continuidad del negocio.

Comité Institucional de Gestión y Desempeño	
Funciones en la administración	1. Minimizar el impacto en la UIAF ante una crisis, aplicando e implementando los procedimientos definidos en la Entidad; 2. Revisar y aprobar las políticas, metodología y planes definidos por la UIAF para la gestión de continuidad del negocio; 3. Aprobar y realizar seguimiento a la continuidad del negocio de acuerdo con las políticas y estrategias definidas; 4. Identificar los interesados claves que deben ser informados sobre el desarrollo o tratamiento de las situaciones de crisis; 5. Comunicar a la entidad la decisión de activar el plan de continuidad de negocio; 6. Actualizar la información de contacto de los miembros del comité; 7. Definir la estrategia frente a la situación de crisis; 8. Aprobar el plan de capacitación en continuidad de negocio propuesto por el líder de este proceso; 9. Supervisar la activación, recuperación, y regreso a la normalidad, tanto la gestión de continuidad como la gestión de los diferentes tipos de incidentes y mantener la efectividad de dichos planes en el tiempo; 10. Aprobar la estructura de gobierno de continuidad; 11. Aprobar las funciones y responsabilidades de todos los que participan en el proceso de continuidad del negocio; 12. Suministrar orientación estratégica; 13. Aprobar los resultados del Análisis de Impacto al Negocio (BIA); 14. Aprobar los Planes de Continuidad.

Fuente: Roles y responsabilidades continuidad de negocio UIAF

5.2. Responsable de Seguridad Digital

La entidad debe designar un responsable de Seguridad Digital, y a su vez el encargado de la Seguridad de la Información, perteneciente a un área que haga parte de la Alta Dirección o Línea Estratégica dando cumplimiento con los compromisos que debe cumplir frente a la gestión del riesgo de seguridad digital tal cual lo establece la Guía para la Administración del Riesgo y el diseño de controles para las entidades públicas Versión 6 de 2022.

6. POLÍTICA DE ADMINISTRACIÓN DEL RIESGO

La Unidad de Información y Análisis Financiero-UIAF, se compromete a establecer y mantener acciones efectivas con la participación de sus servidores públicos, contratistas y proveedores de la entidad encaminadas a mitigar la posibilidad de materialización de las situaciones de amenaza de aquellos eventos

internos o externos que puedan afectar el logro de los objetivos institucionales, sus productos y servicios en el cumplimiento de su misión y visión.

6.1 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, Ley 1762 del 6 de julio de 2015, Decreto 152 y 153 del 28 de enero de 2022, Resolución 196 del 19 de Julio de 2022, Resolución 26 de 23 de enero de 2023, desempeñándose 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, y delitos ambientales.

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

6.1.1. Propósito Superior

Proteger los derechos humanos, prevenir y combatir los diferentes riesgos y amenazas contra el régimen democrático, el régimen constitucional y legal, la seguridad y defensa nacional, la estabilidad económica y social y la construcción de la paz; a través de la persecución de economías criminales, finanzas ilícitas y detección de redes criminales complejas, proyectando a la UIAF como cabeza del Sistema ALA/CFT/CFP a nivel país, como un líder regional y un referente internacional.

6.1.2. Misión

Hacemos productos de inteligencia financiera de carácter orientador fundamentados en metodologías de rigor científico para prevenir y detectar amenazas que afecten la economía nacional.

6.1.3. Visión

Seremos reconocidos a nivel mundial por nuestra innovación y efectividad como el referente entre los organismos de inteligencia financiera.

6.1.4. Líneas de Acción, Objetivos Estratégicos y Estrategias

a) Línea de Acción 1. – Prevención

Objetivo Estratégico: Aumentar la efectividad en la prevención del lavado de activos y el financiamiento del terrorismo y el financiamiento de la proliferación de armas de destrucción masiva.

Estrategia 1.1. Fortalecer el conocimiento y la cultura antilavado en todos los actores del Sistema ALA/CFT/CFP.
Estrategia 1.2. Crear tanques de pensamiento para fortalecer el entendimiento de temas relacionados con LA/FT/FP.
Estrategia 1.3. Optimizar y desarrollar la herramienta tecnológica de la Evaluación Nacional del Riesgo - ENR Digital versión 2.0 en el 2025.

Estrategia 1.4. Proponer política pública tendiente a robustecer el funcionamiento del Sistema ALA/CFT/CFP del país.
Estrategia 1.5 Generar conocimiento en economías criminales, fenómenos económicos y entendimiento de LA/FT/FP.
Estrategia 1.6. Estructuración del Sistema de Información y Análisis contra finanzas provenientes de delitos ambientales y de corrupción, como lo dispone el Plan Nacional de Inteligencia y el Plan Nacional de Desarrollo.

b) Línea de Acción 2. – Detección

Objetivo Estratégico: Detectar e identificar las redes criminales de LA/FT/FP nacionales y transnacionales, así como redes de corrupción que desfalcan el patrimonio del Estado; además, de organizaciones criminales que atentan contra el medio ambiente.

Estrategia 2.1. Fortalecer el trabajo conjunto con la Fiscalía General de la Nación, la Corte Suprema de Justicia y cooperar con organismos de inteligencia nacionales e internacionales y demás actores del Sistema ALA/CFT/CFP y adelantar actividades coordinadas con homólogos u organismos internacionales de similar naturaleza
Estrategia 2.2. Actualizar de manera permanente las fuentes de información.
Estrategia 2.3. Fortalecer la inteligencia financiera como una herramienta para la protección del medio ambiente.
Estrategia 2.4. Fortalecer la inteligencia financiera como una herramienta para la lucha contra la corrupción.
Estrategia 2.5. Fortalecer la inteligencia financiera como una herramienta para la consecución de la Paz Total.

c) Línea de Acción 3. - Transformación Tecnológica e Innovación

Objetivo Estratégico: Implementar proyectos de modernización tecnológica que soporten la misionalidad, apalancándose en herramientas innovadoras.

Estrategia 3.1. Dinamizar el acceso a la información requerida por la entidad.
Estrategia 3.2. Fortalecer las herramientas tecnológicas de recepción, almacenamiento, procesamiento, análisis e intercambio de información.
Estrategia 3.3. Mejorar y optimizar la capacidad de almacenamiento y procesamiento de la información.
Estrategia 3.4 Actualizar y optimizar las aplicaciones utilizadas para la generación de los informes de inteligencia.
Estrategia 3.5. Robustecer el proceso de seguridad de la información.
Estrategia 3.6 Dimensionar los requerimientos y recursos tecnológicos y de seguridad que se deriven de la regionalización.

d) Línea de Acción 4. - Articulación y cooperación a nivel nacional e internacional

Objetivo Estratégico:
Coordinar acciones con las entidades a nivel nacional e internacional que potencien las capacidades de la UIAF.

Estrategia 4.1.
Fortalecer el relacionamiento nacional e internacional a través de convenios de cooperación, memorandos de entendimiento y acuerdos de intención.

Estrategia 4.2. Coordinar con las entidades competentes la presentación de un marco normativo pertinente para mejorar la calificación del país en la quinta ronda de evaluaciones mutuas del GAFILAT

e) Línea de Acción 5. - UIAF como UIF líder en el Mundo

Objetivo Estratégico: posicionar a la UIAF como una UIF referente a nivel regional y mundial, mediante la coordinación de acciones con las entidades pertinentes para preparar al país de cara a la quinta ronda de evaluaciones mutuas del GAFILAT y obtener una mejor calificación en las 40 recomendaciones del GAFI.

Estrategia 5.1. Compartir las buenas prácticas de la UIAF con homólogos de la región.
Estrategia 5.2. Mantener y fortalecer la participación de la UIAF en la plenaria y grupos de trabajo del Grupo Egmont.
Estrategia 5.3. Fortalecer la relación con las UIF de la región, mediante el intercambio de información.
Estrategia 5.4. Fortalecer las capacidades de la UIAF a través de asistencia técnica y herramientas de vanguardia.
Estrategia 5.5. Formular proyectos regionales en el marco de la cooperación con otras UIF.
Estrategia 5.6. Desarrollar acciones para superar las deficiencias priorizadas por el país identificadas en el Informe de Evaluación Mutua (IEM) de GAFILAT de 2018.

f) Línea de Acción 6. - Regionalización

Objetivo Estratégico: lograr que la inteligencia financiera llegue a todas las regiones del país.

Estrategia 6.1. Realizar convenios con entidades territoriales y descentralizadas.
Estrategia 6.2. Identificar las zonas vulnerables por medio de estudios estratégicos.
Estrategia 6.3. Realizar capacitaciones y acompañamientos a las regiones más afectadas por las acciones de las organizaciones multicrimen asociadas a ALA/FT/FP y corrupción.

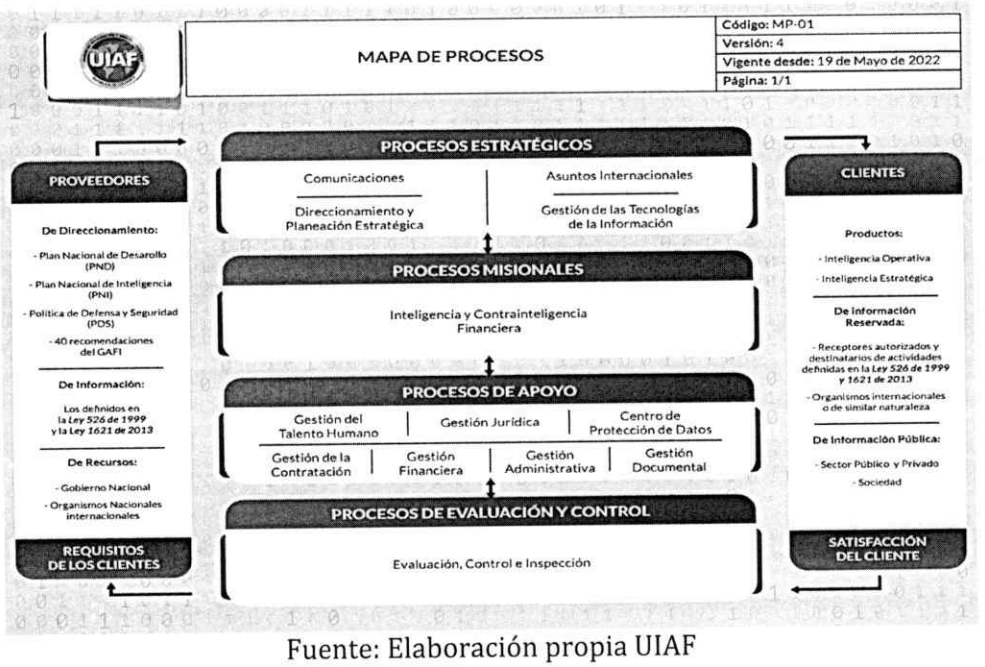
g) Línea de Acción 7. - Gestión y Desempeño Institucional

Objetivo Estratégico: Incrementar la capacidad de apoyo a las áreas misionales y de desempeño institucional, optimizando los recursos físicos, humanos, financieros y la eficiencia y calidad en el desarrollo de sus procesos.

Estrategia 7.1. Adelantar un proceso de rediseño organizacional de la estructura y planta de personal.
Estrategia 7.2. Gestionar la consecución de recursos que permita ampliar la capacidad de la infraestructura física.
Estrategia 7.3. Fomentar la mejora continua a través del seguimiento y la evaluación del desempeño institucional.
Estrategia 7.4. Generar espacios de innovación y gestión del conocimiento, que fortalezcan las competencias del talento humano, desarrollo de ideas innovadoras y aplicación de lecciones aprendidas.
Estrategia 7.5. Implementar mejores prácticas para la correcta gestión de los documentos y la información
Estrategia 7.6. Contar con funcionarios competentes, comprometidos y con altos niveles de productividad y satisfacción que contribuyan al mejoramiento institucional.

6.2.5. Mapa de Procesos

Ilustración 1. Mapa de procesos UIAF



Fuente: Elaboración propia UIAF

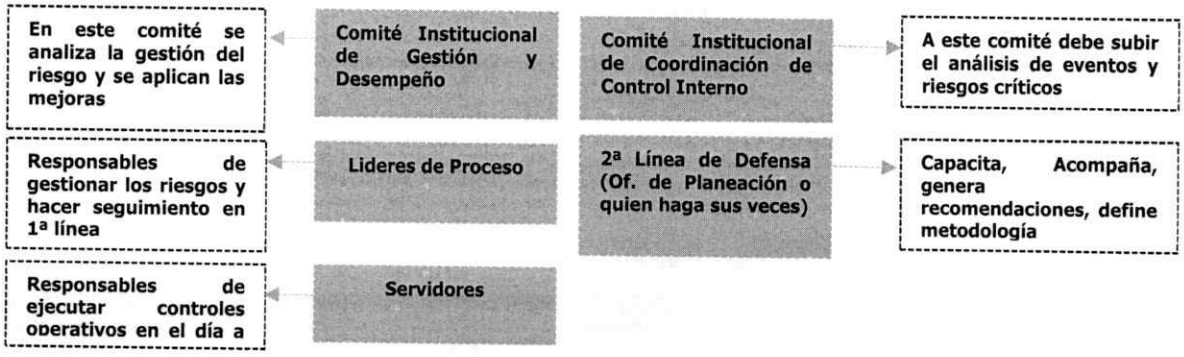
7. METODOLOGÍA

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 6, noviembre de 2022.

De igual manera, se incorporan los lineamientos definidos en el Manual Operativo del Modelo Integrado de Planeación y Gestión– MIPG Versión 5, la Guía para la identificación y declaración del conflicto de intereses en el Sector Público colombiano, emitida por el DAFP en el año 2019.

De otra parte, el Modelo Integrado de Planeación y Gestión (MIPG), define para su operación y articula 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:

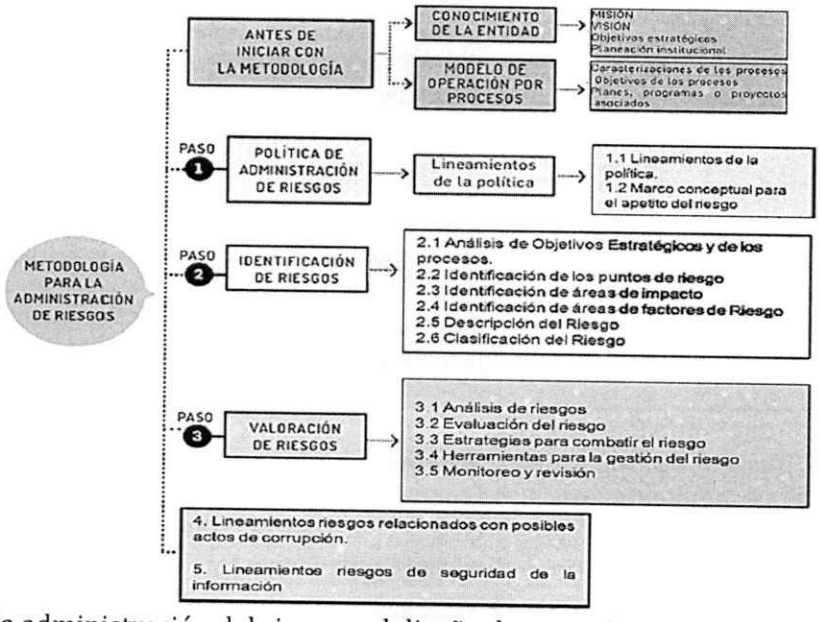
Ilustración 2. Marco general para la gestión del riesgo



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas - versión 6

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:

Ilustración 3. Metodología para la administración de riesgos



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas - versión 6

7.1. 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), el cual hace parte del Marco Estratégico Institucional que direccionará a la entidad.

Factores de Riesgo en Seguridad Digital

Se deben considerar los siguientes factores:

Tabla 3. 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.	Identificación de los procesos y su respectiva caracterización.
Entorno cultural.	Empleados, contratistas.	Flujos de información.
Cualquier otro factor externo de tipo internacional, nacional (gobierno), regional o local.	La misión, visión, principios, valores y lema 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 mediante el 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 digital, 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.

Factores Externos	Factores Internos	Factores de los Procesos
	Sistemas de información o servicios.	Procesos de gestión de riesgos que se tienen actualmente implementados.
		Personal involucrado en la toma de decisiones.

Fuente: Lineamientos para la gestión de riesgos de seguridad digital en entidades públicas

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.

Establecimiento del Contexto para la Gestión de los Riesgos Ambientales

Es importante garantizar que en los objetivos definidos para el proceso de gestión de riesgo se tomen en consideración el ambiente externo y el organizacional.

7.2. 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:** Los riesgos que se identifiquen deben tener impacto en el cumplimiento del objetivo estratégico o del proceso.
- **Identificación de los Puntos de Riesgo:** Actividades dentro del flujo del proceso donde 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:** 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:** Fuentes generadoras de riesgos.

Tabla 4. Factores de riesgos

Factor	Definición		Descripción
Procesos	Eventos relacionados con errores en las actividades que deben realizar los servidores de la organización.		Falta de procedimientos
			Errores de grabación, autorización
			Errores en cálculos para pagos interno y externos
			Falta de capacitación, temas relacionados con el personal

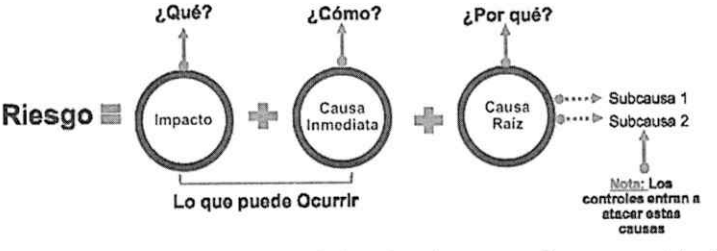
Talento Humano	Incluye seguridad y salud en el trabajo. Se analiza posible dolo e intención frente a la corrupción		Hurto activos
			Posibles comportamientos no éticos de los empleados
			Fraude interno (corrupción, soborno)
Tecnología	Eventos relacionados con la infraestructura tecnológica de la entidad		Daño de equipos
			Caída de aplicaciones
			Caída de redes
			Errores en programas
Infraestructura	Eventos relacionados con la infraestructura física de la entidad		Derrumbes
			Incendios
			Inundaciones
			Daños a activos
Evento Externo	Situaciones externas que afectan la entidad		Suplantación de identidad
			Asalto a la oficina
			Atentados, vandalismo, orden público

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas - versión 6

a. Descripción del Riesgo

Debe contener 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:

Ilustración 4. Descripción del riesgo



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas - versión 6

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:** 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 es posible que exista más de una causa o subcausas que serían 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.

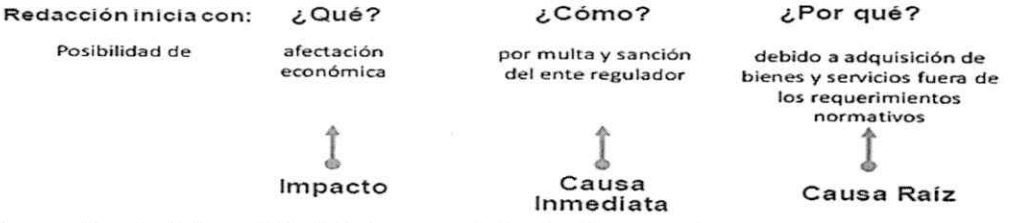
- No describir causas como riesgos.
  Ejemplo: inadecuado funcionamiento de la plataforma estratégica donde se realiza el seguimiento a la planeación.

- 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.

Ilustración 5. Ejemplo aplicado bajo la estructura propuesta para la redacción del riesgo



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas - versión 6

b. Descripción del Riesgo Fiscal

Para la redacción del riesgo fiscal es importante identificar la causa raíz o potencial hecho generador del daño.

Para redactar un riesgo fiscal se debe tener en cuenta:

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

Ejemplo:

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

Ilustración 6. Descripción del riesgo fiscal

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas - versión 6

Tabla 5. Redacción del riesgo fiscal

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

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas - versión 6

Tabla 6. Ejemplos acordes con el objeto sobre el que recae el efecto dañoso

Bienes Públicos	Recursos Públicos	Intereses Patrimoniales de Naturaleza Pública
Posibilidad de efecto dañoso sobre bienes públicos, por daño	Posibilidad de efecto dañoso sobre los recursos públicos,	Posibilidad de efecto dañoso sobre intereses patrimoniales de naturaleza

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

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas - versión 6

Clasificación del Riesgo

Permite agrupar los riesgos identificados, se clasifica cada uno de los riesgos en las siguientes categorías:

Tabla 7. Clasificación de los riesgos

Clase	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 están 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.
Conflicto de Intereses	Falta de integridad, honestidad y responsabilidad de los funcionarios públicos.
Continuidad del Negocio	Incumplimiento en las metas y objetivos institucionales afectando el cumplimiento en las metas de gobierno.

Clase	Descripción
Datos Personales	Robo de la identidad, vulneración sexual, violencia de género, pérdidas económicas, daños a bienes y pérdida del empleo o de oportunidades comerciales o profesionales.
Seguridad y Salud en el Trabajo	Niveles de exposición a los peligros identificados en la Entidad.
Ambiental	Efectos en el impacto ambiental.

Fuente: Guía para administración del riesgo y diseño de controles en entidades públicas - versión 6 - Propias UIAF– ISO 22301

7.2.1. Identificación de Riesgos Fiscales

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

Es importante resaltar que, por cada punto de riesgo fiscal, existen múltiples circunstancias inmediatas.
Para poder identificar los puntos de riesgo y las circunstancias inmediatas, se sugiere realizar un taller en la entidad donde involucre al nivel directivo y funcionarios de las diferentes áreas para que se identifique los puntos de riesgo fiscal y circunstancias inmediatas.

Tabla 8. Preguntas orientadoras para los puntos de riesgo fiscal y causa inmediatas

Sirve para Identificar	Preguntas y Respuestas para Identificación
Puntos de riesgo fiscal	¿En qué procesos de la entidad se realiza gestión?
Puntos de riesgo fiscal y circunstancias inmediatas	Clasifique por procesos (según mapa de procesos de la entidad), hallazgos con presunta incidencia fiscal identificados por el ente de control fiscal y/o los fallos con responsabilidad fiscal en firme relacionados con hechos de la entidad o del sector y/o las advertencias de la Contraloría General de la República y/o las alertas reportadas en el Sistema de Alertas de Control Interno -SACI. Nota 1: para este efecto se recomienda consultar los hallazgos con presunta incidencia fiscal y los fallos con responsabilidad fiscal de los últimos 5 años. Nota 2: los hallazgos fiscales de los últimos años y las advertencias que se hayan emitido en relación con la gestión fiscal de la entidad, se obtienen de la matriz de plan de mejoramiento institucional y de los históricos, información con la que cuenta la Oficina de Control Interno o quien haga sus veces.

Sirve para Identificar	Preguntas y Respuestas para Identificación
	Nota 3: Los fallos con responsabilidad fiscal en firme son información pública, a la cual se puede acceder mediante solicitud de información y documentos (derecho de petición) ante el o los entes de control fiscal que vigilen a la entidad respectiva o al sector que esta pertenece. Estos precedentes son muy importantes para conocer la causa raíz (hechos generadores) por los que se ha fallado con responsabilidad en los últimos años y así implementar los controles adecuados para atacar de forma preventiva esas causas y evitar efectos dañosos sobre los recursos, bienes o intereses patrimoniales del estado. Nota 4: La organización y agrupación por procesos (según el mapa de procesos de la entidad) de los hallazgos con presunta incidencia fiscal identificados por el ente de control fiscal, los fallos con responsabilidad fiscal en firme relacionados con hechos de la entidad o del sector, las advertencias de la Contraloría General de la República y las alertas reportadas en el Sistema de Alertas de Control Interno -SACI, es una labor de la segunda línea de defensa, específicamente de la Oficina de Planeación o quien haga sus veces, con la asesoría de la Oficina de Control Interno o quien haga sus veces.
Circunstancias inmediatas	En un ejercicio autocritico, realista y objetivo, ¿Cuáles son las causas de los hallazgos fiscales identificados por el ente de control fiscal y/o de los fallos con responsabilidad fiscal relacionados con hechos de la entidad o del sector y/o las advertencias de la oficina de control interno, en los últimos 3 años? Nota: se recomienda no copiar las causas escritas por el órgano de control en el hallazgo, salvo que luego del análisis propio la entidad concluya que la causa de hallazgo es la identificada por el órgano de control.
Puntos de riesgo fiscal y circunstancias inmediatas	¿Qué puntos de riesgo fiscal y circunstancias inmediatas del ¿Catálogo Indicativo y Enunciativo de Puntos de riesgo fiscal y circunstancias Inmediatas son aplicables a la entidad?

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas - versión 6

7.2.2. Identificación Riesgos de Seguridad y Salud en el Trabajo

Identificación de los Peligros

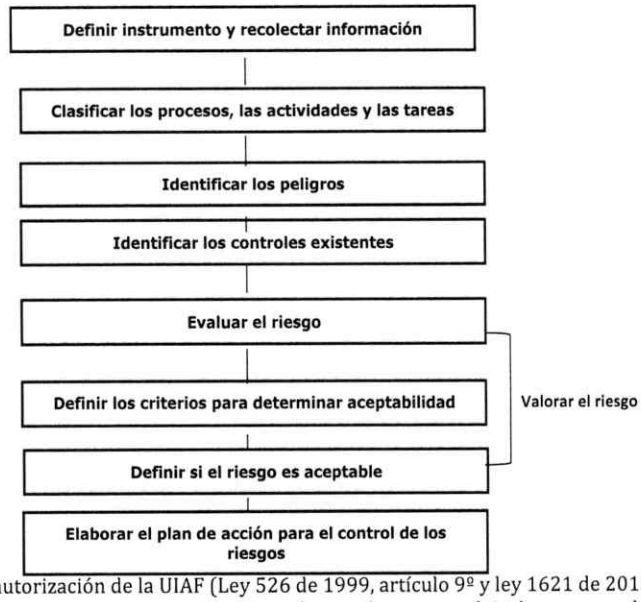
El propósito general de la identificación es entender los peligros que se pueden generar en el desarrollo de las actividades, con el fin que la entidad pueda establecer los controles necesarios, al punto de asegurar que cualquier riesgo sea aceptable.

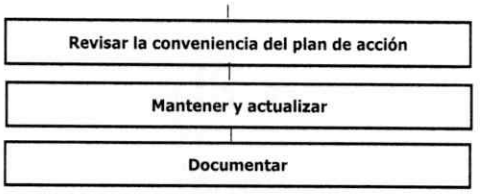
Aspectos a Tener en Cuenta para Desarrollar la Identificación de los Peligros

Las siguientes actividades son necesarias para que las organizaciones realicen la identificación de los peligros de los riesgos:

- **Definir el Instrumento para Recopilar la Información**: una herramienta donde se registre la información para la identificación de peligros y valoración de los riesgos.
- **Clasificar los Procesos, Actividades y las Tareas:** preparar una lista de los procesos de trabajo y de cada una de las actividades que lo componen y clasificarlas; esta lista debería incluir instalaciones, planta, personas y procedimientos.
- **Identificar los Peligros**: incluir todos aquellos relacionados con cada actividad laboral. Considerar quién, cuándo y cómo puede resultar afectado.
- **Identificar los Controles Existentes**: relacionar todos los controles que la organización ha implementado para reducir el riesgo asociado a cada peligro.
- **Elaborar el Plan de Acción**: para el control de los riesgos, con el fin de mejorar los controles existentes si es necesario, o atender cualquier otro asunto que lo requiera.
- **Revisar la Conveniencia del Plan de Acción**: re-valorar los riesgos con base en los controles propuestos y verificar que los riesgos serán aceptables.
- **Mantener y Actualizar**:
  - Realizar seguimiento a los controles nuevos y existentes y asegurar que sean efectivos;
  - Asegurar que los controles implementados sean efectivos y que la valoración de los riesgos está actualizada.
- **Documentar**: el seguimiento a la implementación de los controles establecidos en el plan de acción que incluya responsables, fechas de programación, ejecución y estado actual como parte de la trazabilidad de la gestión en la seguridad y salud en el trabajo.

Tabla 9. Identificación de los peligros y la valoración de los riesgos





Fuente: Guía para la identificación de peligros y la valoración de los riesgos en seguridad y salud ocupacional – GTC 45

Definir el Instrumento para Recolectar Información

Las organizaciones deberían contar con una herramienta para consignar de forma sistemática la información proveniente del proceso de la identificación de los peligros y la valoración de los riesgos, la cual debería ser actualizada periódicamente:

Tabla 10. Información proveniente del proceso de la identificación de los peligros y la valoración de los riesgos

Proceso
Zona / Lugar
Actividades
Tareas
Rutinaria (Si o No)
Peligro
Descripción
Clasificación
Efectos posibles
Controles existentes: -Fuente -Medio -Individuo
Evaluación del riesgo -Nivel de deficiencia; -Nivel de exposición; -Nivel de probabilidad (NP= NDxNE); -Interpretación del nivel de probabilidad -Nivel de consecuencia -Nivel de Riesgo (NR) e Intervención, e Interpretación nivel de riesgo
Valoración del riesgo: - Aceptabilidad del riesgo
Criterios para establecer controles: -Número de expuestos -Peor consecuencia -Existencia de requisitos legal especifico asociado (Si o no)
Medidas de intervención:

-Eliminación -Sustitución -Controles de Ingeniería -Controles administrativos, señalización, advertencia y Equipos/elementos de protección personal

Fuente: Guía para la identificación de los peligros y la valoración de los riesgos en seguridad y salud ocupacional – GTC 45

Descripción y Clasificación de Peligros

Para identificar los peligros, se recomienda plantear una serie de preguntas como las siguientes:

- ¿existe una situación que pueda generar daño?
- ¿Quién (o qué) puede sufrir daño?
- ¿Cómo puede ocurrir el daño?
- ¿Cuándo puede ocurrir el daño?

La entidad deberá desarrollar su propia lista de peligros tomando en cuenta el carácter de sus actividades laborales y los sitios en que se realiza el trabajo.

7.2.3. Identificación Riesgo Ambiental

Esta etapa busca identificar los riesgos que se van a gestionar. Es esencial realizar una identificación de conjunto usando un proceso sistemático bien estructurado, debido a que un riesgo potencial no identificado en esta etapa se excluirá del análisis posterior. La identificación debe incluir todos los riesgos, estén o no bajo control de la organización (Tomado de la Gestión del Riesgo Ambiental Principios y Procesos – GTC 104).

Cómo Identificar los Riesgos

La identificación de los riesgos ambientales se produce en varias etapas. Inicialmente, se identifican los problemas y aspectos ambientales tanto en el área estratégica como en la operativa o a nivel del proyecto. En consecuencia, un examen más detallado debería tener en cuenta los ecosistemas naturales, el medio ambiente general, los pueblos y comunidades, y los negocios (Tomado de la Gestión del Riesgo Ambiental Principios y Procesos – GTC 104).

Las siguientes etapas proporcionan una guía práctica de la manera en que se deben identificar las fuentes de riesgo y los impactos ambientales potenciales:

- Identificar las fuentes de riesgo: implica la identificación de peligros, aspectos ambientales e incidentes potenciales que pueden suceder.
- Describir el ambiente circundante.
- Identificar los impactos ambientales potenciales.

Tabla 11. Ejemplo tipos de fuentes de impactos

Fuente		Ruta	Barrera	Receptor	Impacto
Peligro/aspecto	Evento				
Fuente de energía: -Química -Eléctrica -Mecánica -Por presión -Por ruido -Por gravedad -Calor y frío -Radiación -Biomecánica -Microbiológica Maquinaria Procesos -Actividades Inventario de materias primas e insumos	Falla de planta. Liberación tóxica. Fuego Contaminación Limpieza de la tierra Actividades de dragado Disposición de desechos	Dispersión y deposición atmosférica. Superficie acuática: -Drenaje local y escurrimiento, -Corrientes y sistemas, hidrológicos, Aguas, Subterráneas, Suelo, Rutas biológicas: -Ingestión -Cadena alimentaria -Vectores biológicos	Física De Procesamiento Administrativa Reglamentaria	Humano Social Económico Instalaciones Patrimonio Natural Patrimonio cultural	Medidas relacionadas con: -Sostenibilidad -Seres Humanos -Sociedad -Economía -Instalaciones - Patrimonio natural -Patrimonio cultural

Fuente: Gestión del riesgo ambiental principios y procesos – GTC 104

Definición Riesgo Ambiental: se debería considerar como las consecuencias ambientales de una gravedad determinada y la probabilidad de que presente esa consecuencia particular.

Cómo identificar los riesgos

Fuente de Riesgo: incluye todas las fuentes de un riesgo cuando existe una relación causa-efecto, así como los términos "Peligros" "aspectos ambientales", "incidentes" y eventos".

La fuente de riesgo también puede incluir problemas ambientales que pueden producir consecuencias para los negocios de la organización (Tomado de la Gestión del Riesgo Ambiental Principios y Procesos – GTC 104).

Análisis de los Riesgos

El análisis del riesgo ambiental involucra con frecuencia muchas disciplinas, dentro de las que se encuentran la ingeniería, la ecotoxicología, la hidrogeología y las ciencias biológicas y sociales. Para llevar a cabo el trabajo se debería utilizar especialistas que tengan la mezcla pertinente de habilidades profesionales y es necesario

que se entiendan mutuamente. También que se planifique y tenga en cuenta los recursos para planificación y consulta entre los diferentes especialistas involucrados en un proyecto (Tomado de la Gestión del Riesgo Ambiental Principios y Procesos – GTC 104).

Implementación del Plan de Comunicación del Riesgo Ambiental

Se recomienda Planificar e iniciar la comunicación lo más pronto posible, particularmente cuando parece posible que las actividades de una organización involucran el interés del público. Se debe implementar medios de comunicación y consulta con las partes interesadas y entre ellas como parte del proceso de asegurar que todas estén involucradas e informadas en un nivel apropiado.

El plan de comunicación y consulta se debería monitorear y revisar de la misma manera que el proceso de gestión del riesgo, para asegurar que cumplen los objetivos especificados cuando se estableció el contexto.

7.2.4. Identificación de los Riesgos de Conflictos de Intereses

Definición de Conflicto de Intereses: el servidor público tiene intereses privados que podrían influir indebidamente en la actuación de sus funciones y sus responsabilidades oficiales. Se contempla la materialización del conflicto de intereses al precisar que el interés privado "en efecto influye" en la toma de decisiones (Tomado de la guía para la identificación y declaración del conflicto de intereses en el sector público colombiano- versión 2).

Tipos de Conflicto de Intereses

Aparente: cuando el servidor público no tiene un interés privado, pero alguien podría llegar a concluir, aunque sea de manera tentativa, que sí lo tiene. Una forma práctica de identificar si existe un conflicto de intereses aparente es porque el servidor puede ofrecer toda la información necesaria para demostrar que dicho conflicto no es ni real ni potencial (Tomado de la guía para la identificación y declaración del conflicto de intereses en el sector público colombiano-versión 2).

Potencial: cuando el servidor tiene un interés particular que podría influir en sus obligaciones como servidor público, pero aún no se encuentra en aquella situación en la que debe tomar una decisión. No obstante, esta situación podría producirse en el futuro.

Real: cuando el servidor ya se encuentra en una situación en la que debe tomar una decisión, pero, en el marco de esta, existe un interés particular que podría influir en sus obligaciones como servidor público. Por ello, se puede decir que este tipo de conflicto son riesgos actuales.

Tabla 12. Tipos de conflicto de interés

	Real	Potencial	Aparente
Interés particular	Tengo un **interés particular** que podría influir en mis obligaciones como servidor público		**No tengo interés particular** que pueda influir en mis obligaciones como servidor público
Decisión profesional del servidor público	Ya estoy en una situación en la que tengo que tomar la decisión	Aún no estoy en la situación en la que tengo que tomar la decisión, pero esta podría producirse en el futuro	Ya estoy en la situación de tomar una decisión y alguien podría razonablemente pensar que tengo un interés que podría influir

Fuente: Identificación declaración conflicto intereses Departamento Administrativo de la Función Pública-DAFP

Tipificación del Conflicto de Intereses Según la Normativa Colombiana

Cuyo propósito es aclararle a los servidores aquellas situaciones del conflicto en las cuales deben efectuar una declaración de impedimento:

Tabla 13. Tipificación de situaciones de conflicto de intereses según la normativa colombiana

Tipo	Descripción	Aplica a parientes/ grados/terceros (socios)	Fuente normativa
Interés directo/ conocimiento previo/concepto o consejo fuera de la actuación	Que el servidor tenga interés particular y directo en la regulación, gestión, control o decisión del asunto.	Que el interés particular y directo o el conocimiento previo del asunto lo tengan el cónyuge, compañero o compañera permanente del servidor o alguno de sus parientes dentro del cuarto grado de consanguinidad (hijos, padres, hermanos, abuelos, nietos, tíos, sobrinos, primos), segundo de afinidad (suegros y cuñados) o primero civil (padre adoptante o hijo adoptivo), o su socio o socios de hecho o de derecho.	C.P. art 126 Ley 1437 de 2011, art.11 numeral 1 Ley 734 de 2002, art. 84 numeral 1 Ley 1564 de 2012, art.141 numeral 1 Ley 136 de 1994, art. 70 Ley 5 de 1992, art. 286
	Que el servidor haya conocido del asunto en oportunidad anterior.		Ley 1437 de 2011, art.11 numeral 2 Ley 1564 de 2012, art.141 numeral 2
	Que el servidor haya dado consejo o concepto por fuera de la actuación administrativa sobre las cuestiones materia de la misma, o haya intervenido en esta como apoderado, agente del ministerio público, perito o testigo (no tendrán el carácter de concepto las referencias o explicaciones que el servidor público haga sobre el contenido de una decisión tomada por la administración).		Ley 1437 de 2011, art.11 numeral 11 Ley 734 de 2002, art. 84 numeral 4 Ley 1564 de 2012, art.141 numeral 12
	Que el servidor haya proferido la decisión que está sujeta a su revisión.		Ley 734 de 2002, art. 84 numeral 2

Tipo	Descripción	Aplica a parientes/ grados/terceros (socios)	Fuente normativa
Curador o tutor del interesado	Que el servidor sea curador o tutor de persona interesada en el asunto.	Que el cónyuge, compañero permanente o alguno de sus parientes arriba indicados del servidor, sea curador o tutor de persona interesada en el asunto.	Ley 1437 de 2011, art.11 numeral 3 Ley 1564 de 2012, art.141 numeral 4
Relación con las partes	Que el servidor tenga relación con las partes interesadas en el asunto.	Ser cónyuge, compañero permanente o pariente de alguna de las partes o de su representante o apoderado, dentro del cuarto grado de consanguinidad (hijos, padres, hermanos, abuelos, nietos, tíos, sobrinos, primos) o civil (padre adoptante o hijo adoptivo), o segundo de afinidad (suegros y cuñados).	Ley 734 de 2002, art.84, numeral 3 Ley 1564 de 2012, art.141 numeral 3
Amistad o enemistad	Que exista enemistad grave por hechos ajenos a la actuación administrativa, o amistad entrañable entre el servidor y alguna de las personas interesadas en la actuación administrativa, su representante o apoderado.		Ley 1437 de 2011, art.11 numeral 8 Ley 734 de 2002, art.84 numeral 5 Ley 1564 de 2012, art.141 numeral 9
Organización, sociedad o asociación a la cual perteneció o continúa siendo miembro	Que el servidor sea socio de alguna de las personas interesadas en la actuación administrativa o su representante o apoderado en sociedad de personas.	Ser cónyuge, compañero permanente o alguno de los parientes del servidor, socio de alguna de las personas interesadas en la actuación administrativa o su representante o apoderado en sociedad de personas.	Ley 1437 de 2011, art.11 numeral 10 Ley 734 de 2002, art.84, numeral 6 Ley 1564 de 2012, art.141 numeral 11

Tipo	Descripción	Aplica a parientes/ grados/terceros (socios)	Fuente normativa
Litigio o controversia/ decisión administrativa pendiente	Que exista litigio o controversia ante autoridades administrativas o jurisdiccionales entre el servidor y cualquiera de los interesados en la actuación, su representante o apoderado.	Que exista litigio o controversia ante autoridades administrativas o jurisdiccionales entre el cónyuge, compañero permanente, o alguno de los parientes del servidor y cualquiera de los interesados en la actuación, su representante o apoderado.	Ley 1437 de 2011, art.11 numeral 5 Ley 1564 de 2012, art.141 numeral 6
	Que el servidor tenga decisión administrativa pendiente en que se controvierta la misma cuestión jurídica que él debe resolver.	Tener el cónyuge, compañero permanente o alguno de los parientes en segundo grado de consanguinidad (hijos, padres, hermanos, abuelos, nietos) o primero civil (padre adoptante o hijo adoptivo del servidor, decisión administrativa o pleito pendiente en que se controvierta la misma cuestión jurídica que él debe resolver.	Ley 1437 de 2011, art.11 numeral 13 Ley 1564 de 2012, art.141 numeral 14

Tipo	Descripción	Aplica a parientes/ grados/terceros (socios)	Fuente normativa
Denuncia penal o disciplinaria	Que alguno de los interesados en la actuación, su representante o apoderado, haya formulado denuncia penal o disciplinaria contra el servidor, antes de iniciarse la actuación administrativa; o después, siempre que la denuncia se refiera a hechos ajenos a la actuación y que el denunciado se halle vinculado a la investigación penal o disciplinaria.	Que alguno de los interesados en la actuación, su representante o apoderado haya formulado denuncia penal o disciplinaria contra el cónyuge, compañero permanente del servidor o su pariente hasta el segundo grado de consanguinidad (hijos, padres, hermanos, abuelos, nietos), segundo de afinidad (suegros y cuñados) o primero civil (padre adoptante o hijo adoptivo), antes de iniciarse la actuación administrativa; o después, siempre que la denuncia se refiera a hechos ajenos a la actuación y que el denunciado se halle vinculado a la investigación penal o disciplinaria.	Ley 1437 de 2011, art.11 numeral 6 Ley 734 de 2002, art. 84, numeral 8 Ley 1564 de 2012, art.141 numeral 7
	Que el servidor haya formulado denuncia penal contra una de las personas interesadas en la actuación administrativa o su representante o apoderado, o estar aquellos legitimados para intervenir como parte civil en el respectivo proceso penal.	Que el cónyuge, compañero permanente o pariente hasta el segundo grado de consanguinidad (hijos, padres, hermanos, abuelos, nietos), segundo de afinidad (suegros y cuñados) o primero civil (padre adoptante o hijo adoptivo) del servidor haya formulado denuncia penal contra una de las personas interesadas en la actuación administrativa o su representante o apoderado, o estar aquellos legitimados para intervenir como parte civil en el respectivo proceso penal.	Ley 1437 de 2011, art.11 numeral 7 Ley 1564 de 2012, art.141 numeral 8

Tipo	Descripción	Aplica a parientes/ grados/terceros (socios)	Fuente normativa
Acreedor/ deudor	Que el servidor sea acreedor o deudor de alguna de las personas interesadas en la actuación administrativa, su representante o apoderado, salvo cuando se trate de persona de derecho público, establecimiento de crédito o sociedad anónima.	Que el cónyuge, compañero permanente o alguno de los parientes en segundo grado de consanguinidad (hijos, padres, hermanos, abuelos, nietos), primero de afinidad (suegros) o primero civil (padre adoptante o hijo adoptivo del servidor, sea acreedor o deudor de alguna de las personas interesadas en la actuación administrativa, su representante o apoderado, salvo cuando se trate de persona de derecho público, establecimiento de crédito o sociedad anónima.	Ley 1437 de 2011, art.11 numeral 9 Ley 734 de 2002, art. 84, numeral 9 Ley 1564 de 2012, art.141 numeral 10
Antiguo empleador	Que el servidor, dentro del año anterior, haya tenido interés directo o haya actuado como representante, asesor, presidente, gerente, director, miembro de Junta Directiva o socio de gremio, sindicato, sociedad, asociación o grupo social o económico interesado en el asunto objeto de definición.		Ley 1437 de 2011, art. 11 numeral 16
Lista de candidatos	Que el servidor haya hecho parte de listas de candidatos a cuerpos colegiados de elección popular inscritas o integradas también por el interesado en el período electoral coincidente con la actuación administrativa o en alguno de los dos períodos anteriores.		Ley 1437 de 2011, art. 11 numeral 14
Recomendación	Que el servidor haya sido recomendado por el interesado en la actuación para llegar al cargo que ocupa o haya sido señalado por este como referencia con el mismo fin.		Ley 1437 de 2011, art. 11 numeral 15

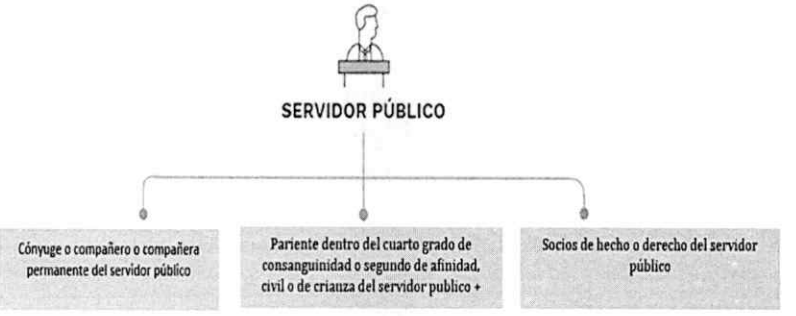
Tipo	Descripción	Aplica a parientes/ grados/terceros (socios)	Fuente normativa
Relación contractual o de negocios	Que alguno de los interesados en la actuación administrativa sea representante, apoderado, dependiente, mandatario o administrador de los negocios del servidor público.		Ley 1437 de 2011, art. 11 numeral 4 Ley 1564 de 2012, art.141 numeral 5
Heredero o legatario	Que el servidor sea heredero o legatario de alguna de las personas interesadas en la actuación administrativa.	Que el cónyuge, compañero permanente o alguno de los parientes del servidor sea heredero o legatario de alguna de las personas interesadas en la actuación administrativa.	Ley 1437 de 2011, art. 11 numeral 12 Ley 734 de 2002, art. 84, numeral 7 Ley 1564 de 2012, art.141 numeral 13
Dádivas	Que el servidor reciba o haya recibido dádivas, agasajos, regalos, favores o cualquier otra clase de beneficios como invitación a desayunar, comer, cenar, a un evento deportivo, de espectáculos, o cualquier otro beneficio incluyendo dinero.		Ley 734 de 2002, art. 35, numeral 3
Participación directa/ asesoría de alguna de las partes interesadas	Que el servidor hubiere participado en la expedición del acto enjuiciado, en la formación o celebración del contrato o en la ejecución del hecho u operación administrativa materia de la controversia.	Que el cónyuge, compañero o compañera permanente, o alguno de los parientes del servidor hasta el segundo grado de consanguinidad (hijos, padres, hermanos, abuelos, nietos), segundo de afinidad (suegros y cuñados) o único civil (padre adoptante o hijo adoptivo) tengan la calidad de asesores o contratistas de alguna de las partes o de los terceros interesados vinculados al proceso, o tengan la condición de representantes legales o socios mayoritarios de una de las sociedades contratistas de alguna de las partes o de los terceros interesados.	Ley 1564 de 2012, art.141 numeral 1 y 4

Tipo	Descripción	Aplica a parientes/ grados/terceros (socios)	Fuente normativa
Relación contractual o de negocios	Que alguno de los interesados en la actuación administrativa sea representante, apoderado, dependiente, mandatario o administrador de los negocios del servidor público.		Ley 1437 de 2011, art. 11 numeral 4 Ley 1564 de 2012, art.141 numeral 5
Heredero o legatario	Que el servidor sea heredero o legatario de alguna de las personas interesadas en la actuación administrativa.	Que el cónyuge, compañero permanente o alguno de los parientes del servidor sea heredero o legatario de alguna de las personas interesadas en la actuación administrativa.	Ley 1437 de 2011, art. 11 numeral 12 Ley 734 de 2002, art. 84, numeral 7 Ley 1564 de 2012, art.141 numeral 13
Dádivas	Que el servidor reciba o haya recibido dádivas, agasajos, regalos, favores o cualquier otra clase de beneficios como invitación a desayunar, comer, cenar, a un evento deportivo, de espectáculos, o cualquier otro beneficio incluyendo dinero.		Ley 734 de 2002, art. 35, numeral 3
Participación directa/ asesoría de alguna de las partes interesadas	Que el servidor hubiere participado en la expedición del acto enjuiciado, en la formación o celebración del contrato o en la ejecución del hecho u operación administrativa materia de la controversia.	Que el cónyuge, compañero o compañera permanente, o alguno de los parientes del servidor hasta el segundo grado de consanguinidad (hijos, padres, hermanos, abuelos, nietos), segundo de afinidad (suegros y cuñados) o único civil (padre adoptante o hijo adoptivo) tengan la calidad de asesores o contratistas de alguna de las partes o de los terceros interesados vinculados al proceso, o tengan la condición de representantes legales o socios mayoritarios de una de las sociedades contratistas de alguna de las partes o de los terceros interesados.	Ley 1564 de 2012, art.141 numeral 1 y 4

Fuente: Identificación declaración conflicto intereses Departamento Administrativo de la Función Pública-DAFP

Cuando Ocurre el Conflicto de Intereses: cuando se tiene un interés particular y directo en la regulación, gestión, control o decisión del asunto por parte de alguno de los siguientes sujetos:

Ilustración 7. Conflicto de intereses en servidor público



Fuente: Identificación declaración conflicto intereses Departamento Administrativo de la Función Pública-DAFP

7.2.5. Identificación de los Riesgos Continuidad de Negocio

Definición de Riesgo de Continuidad del Negocio: posibilidad que se puede presentar de manera interna o externa, afectando el normal desarrollo de las actividades.

Amenazas: las fuentes generadoras de eventos en las que se originan las pérdidas por riesgo son amenazas para los procesos. Se entienden como amenazas, factores de riesgo como el recurso humano, los procesos, la tecnología, la infraestructura y los acontecimientos externos.

Tabla 14. Amenazas en la continuidad de negocio

Amenaza
Dependencia de terceras partes
Ausencia de Planes de Continuidad o Planes de Recuperación de Desastres (DRP)
Ausencia de Pruebas de los Planes de Continuidad y/o los Planes de Recuperación de Desastres (DRP)
Errores Humanos en el soporte de los Sistemas de Información
Ausencia de Pruebas de los Planes de Continuidad y/o los Planes de Recuperación de Desastres (DRP)
Mantenimiento inadecuado / inoportuno de los componentes tecnológicos
Errores Humanos en la operación
Ausencia de Planes de Continuidad o Planes de Recuperación de Desastres (DRP)
Errores y/o manipulación en los elementos de la infraestructura tecnológica
Ausencia de Pruebas de los Planes de Continuidad y/o los Planes de Recuperación de Desastres (DRP)
Falla de medios de respaldo y recuperación

Amenaza
Ausencia de Pruebas de los Planes de Continuidad y/o los Planes de Recuperación de Desastres (DRP)
Deficiencia en la capacidad de almacenamiento del correo electrónico
Fallas en el aire acondicionado
Ausencia de sistemas redundantes (Alta Disponibilidad)
Fallas en los componentes tecnológicos
Ausencia de Planes de Continuidad o Planes de Recuperación de Desastres (DRP)
Falta de control en el cumplimiento de estándares de actualización de software
Incapacidad del sistema para atender un alto volumen de conexiones
Implementar planes de DRP y las respectivas pruebas
Ausencia de Pruebas de los Planes de Continuidad y/o los Planes de Recuperación de Desastres (DRP)
Sobrecarga laboral
Ausencia de personal para apoyar proceso de SIG
Software defectuoso
Ausencia de sistemas redundantes (Alta Disponibilidad)
Deficiencia en la capacidad de almacenamiento del correo electrónico
Mantenimiento inadecuado o inoportuno de los componentes tecnológicos
Suplantación de usuarios o Falsificación de derechos de acceso
Ausencia de sistemas redundantes (Alta Disponibilidad)
Temperatura o humedad extremas
Ausencia de Pruebas de los Planes de Continuidad y/o los Planes de Recuperación de Desastres (DRP)

Fuente: Continuidad de negocio plan de recuperación ante desastres – DRP - UIAF

Vulnerabilidades: son las debilidades que puedan evidenciarse en los procesos de negocio o infraestructura tecnológica, las cuales pueden ser explotadas por una amenaza convirtiéndose en un riesgo cuya valoración está determinada por su probabilidad de ocurrencia y el impacto que causa al materializarse.

Tabla 15. Vulnerabilidades en la continuidad de negocio

Vulnerabilidades
Ausencia de sistemas redundantes (Alta Disponibilidad)
Ausencia de personal para apoyar la a implementación del modelo integrado de planeación y gestión
Ausencia de Planes de Continuidad o Planes de Recuperación de Desastres (DRP)
Ausencia de Pruebas de los Planes de Continuidad y/o los Planes de Recuperación de Desastres (DRP)
Deficiencia en la capacidad de almacenamiento del correo electrónico
Falta de control en el cumplimiento de estándares de actualización de software
Incapacidad del sistema para atender un alto volumen de conexiones
Mantenimiento inadecuado o inoportuno de los componentes tecnológicos

Fuente: Continuidad de negocio plan de recuperación ante desastres – DRP – UIAF

7.2.6. 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" (Consejo Nacional de Política Económica y Social —CONPES N° 167 de 2013).

Es importante señalar que sigue vigente los lineamientos sobre los riesgos relacionados con posibles actos de corrupción documentados en el numeral 3.4. Seguimiento de Riesgos de Corrupción de la versión 4 (ratificado en el numeral 5 de la Guía de la Administración del Riesgo y el Diseño de Controles en las Entidades Públicas Versión 6 de 2022).

Tabla 16. Factores de riesgos de corrupción

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 con la Subdirección Administrativa y Financiera y la Oficina Asesora de Planeación)	• 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 (como proceso o bien los procedimientos ligados a este)	• Estudios previos o de factibilidad deficientes. • 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.

Proceso, Procedimiento o Actividad	Factores de Riesgos
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).

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas - versión 4

Para la identificación de riesgos de corrupción, la entidad también puede utilizar fuentes de datos externas como organismos de control y 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:

Tabla 17. Matriz: Definición del riesgo de corrupción

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

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas - versión 6

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

7.2.7. Identificación de los Riesgos de Seguridad Digital

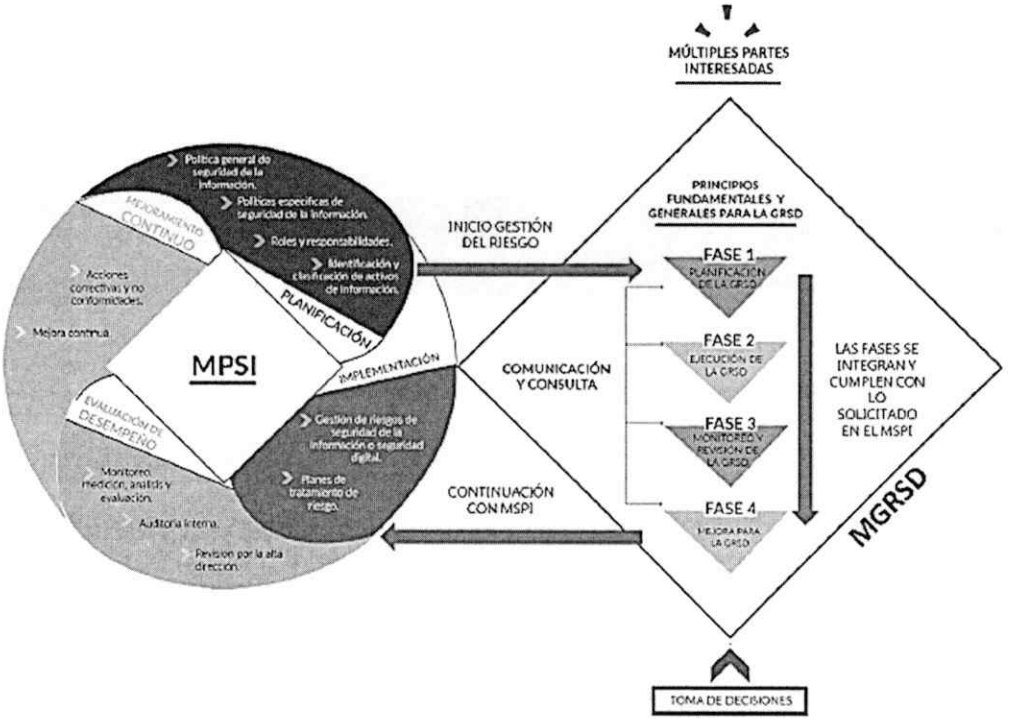
Se debe tener en cuenta que la Política de Seguridad Digital se vincula al Modelo de Seguridad y Privacidad de la Información (MSPI), el cual se encuentra alineado con el Marco de Referencia de Arquitectura TI y soporta transversalmente los otros habilitadores de la política de gobierno digital: Seguridad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

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

- Las actividades de identificación de activos, 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, 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:

Ilustración 8. Modelo de Gestión del Riesgo de Seguridad Digital – MGRSD



Fuente: Lineamientos para la gestión de riesgos de seguridad digital en entidades públicas

Como primer paso para la identificación de los riesgos de seguridad, 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.

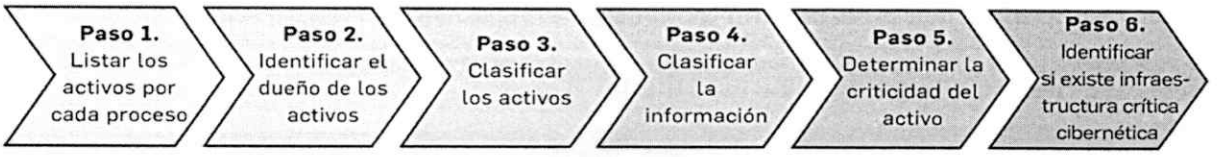
7.2.7.1. Identificación de Activos de Seguridad Digital

Definición de Activo: cualquier elemento que tenga valor para la organización, sin embargo, en el contexto de seguridad digital, son activos: las 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 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.

Ilustración 9. Pasos para la identificación y valoración de activos



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas - versión 6

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 digitales. 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.

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 digital:

- 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. Lineamientos para la gestión de riesgos de seguridad digital en entidades públicas",** donde se encuentran las siguientes tablas necesarias para este análisis:

Tabla 18. Amenazas comunes en seguridad digital

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

Fuente: Lineamientos para la gestión de riesgos de seguridad digital en entidades públicas

Amenazas: Deliberadas (D), Fortuito (F), Ambientales(A), o (E) Externa

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

Tabla 19. 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 Divulgación ilegal de la información	Crimen por computador Acto fraudulento

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

Fuente: Lineamientos para la gestión de riesgos de seguridad digital en entidades públicas

La entidad puede identificar vulnerabilidades (debilidades).

Tabla 20. Vulnerabilidades comunes en seguridad digital

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

Tipo	Vulnerabilidades
	Áreas susceptibles a inundación
	Red eléctrica inestable
	Ausencia de protección en puertas o ventanas
Organización	Ausencia de procedimiento de registro/retiro de usuarios
	Ausencia de proceso para supervisión de derechos de acceso
	Ausencia de control de los activos que se encuentran fuera de las instalaciones
	Ausencia de acuerdos de nivel de servicio (ANS o SLA)
	Ausencia de mecanismos de monitoreo para brechas en la seguridad
	Ausencia de procedimientos y/o de políticas en general (esto aplica para muchas actividades que la entidad no tenga documentadas y formalizadas como uso aceptable de activos, control de cambios, valoración de riesgos, escritorio y pantalla limpia entre otros)

Fuente: Lineamientos para la gestión de riesgos de seguridad digital en entidades públicas

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 logre explotar esa debilidad. Una vulnerabilidad que no tiene una amenaza puede no requerir la implementación de un control.

7.3. 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, porque se puede determinar con claridad la frecuencia con la que se realiza una actividad, en vez de considerar los posibles eventos en el pasado, puesto que, bajo esta óptica si no se ha presentado ningún suceso, 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.

Como referente, se muestran actividades típicas relacionadas con la gestión de una entidad pública, bajo las cuales se definen las escalas de probabilidad.

Tabla 21. Criterios para definir el nivel de probabilidad

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

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas – versión 6

7.3.1. Determinación de la Probabilidad de Ocurrencia

- **Determinación de la Probabilidad de Ocurrencia en Riesgos De Gestión (Seguridad y Salud en el Trabajo, Conflicto de Intereses, Datos Personales), Corrupción y Seguridad Digital:** se 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 puede presentarse, 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.

- **Determinación de la Probabilidad de Ocurrencia en el Riesgo Fiscal:** Se determina según el número de veces que se pasa por el punto de riesgo fiscal en el periodo de 1 año, es decir, el número de veces que se realizan las actividades que representen gestión fiscal.

- **Determinación de la Probabilidad de Ocurrencia en Riesgos Ambientales:** la frecuencia es la tasa de ocurrencia de un efecto, expresada como la cantidad de tales ocurrencias en un tiempo determinado. Por definición, la frecuencia es una medida numérica y se puede usar en enfoques de riesgo cuantitativo. La frecuencia también se puede expresar en otras medidas cuantitativas adecuadas, como es el caso de unidades por millón, por individuos de una población y por miles de nacimientos.

La posibilidad se expresa con un número entre 0 y 1, en donde 0 indica un evento imposible y 1 indica un evento seguro. Por definición la probabilidad es una medida numérica y se puede usar en enfoques de riesgos cuantitativos (Tomado de la Gestión del Riesgo Ambiental Principios y Procesos – GTC 104).

Determinación de la Probabilidad de Ocurrencia en Riesgo de Continuidad Del Negocio: Para calificar la probabilidad de ocurrencia se utilizan los criterios definidos en la siguiente tabla, la cual tiene aplicación tanto para los riesgos de la UIAF (Tomado del documento continuidad de negocio -Plan de Recuperación ante Desastres – DRP).

Tabla 22. Probabilidad de ocurrencia riesgos de continuidad del negocio

Nivel	Descriptor	Descripción	Frecuencia
1	Rara vez	La eventualidad de la ocurrencia es muy baja; casi nula.	No se ha presentado en los últimos 5 años
2	Improbable	Podría ocurrir bajo circunstancias muy excepcionales.	Al menos 1 vez en los últimos 5 años

Nivel	Descriptor	Descripción	Frecuencia
3	Posible	Podría o no ocurrir en algún momento.	Al menos 1 vez en los últimos 2 años
4	Probable	Es viable que el evento ocurra en la mayoría de las circunstancias.	Al menos 1 vez en el último año
5	Casi seguro	Se espera que el evento ocurra en la mayoría de las circunstancias.	Más de 1 vez al año

Fuente: Continuidad de negocio -Plan de Recuperación ante Desastres – DRP- UIAF

7.3.2. Determinación del Impacto o Consecuencia

- **Determinación del Impacto o Consecuencia en Riesgos de Gestión (Seguridad y Salud en el Trabajo, Conflicto de Intereses y Datos Personales):** 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.

Tabla 23. Criterios para definir el nivel de impacto (Riesgos de gestión – Riesgo fiscal)

	Afectación Económica	Reputacional
Leve 20%	Afectación menor a 10 SMLMV	El riesgo afecta la imagen de algún área de la entidad.
Menor 40%	Entre 10 y 50 SMLMV	El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, de junta directiva, funcionarios y/o contratistas.
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 institucionales.
Mayor 80%	Entre 100 y 500 SMLMV	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal.
Catastrófico 100%	Mayor a 500 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país.

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas - versión 6

- **Determinación del Impacto en Riesgo Fiscal:** siempre tendrá un impacto económico, toda vez que el efecto dañoso va a recaer sobre un bien, recurso o interés patrimonial de naturaleza pública. Toda potencial consecuencia económica sobre los bienes, recursos o intereses patrimoniales públicos, es relevante para la adecuada gestión fiscal y prevención de riesgo fiscales. Sin perjuicio de ello, existen diferentes niveles de impacto, según la valoración del potencial efecto dañoso.

  Identificación de Áreas de Impacto: Corresponde a una consecuencia económica sobre el patrimonio público, donde se vería expuesta la Entidad en caso de materializarse el riesgo. No todos los efectos económicos corresponden a riesgos, pero todos los riesgos fiscales (efecto dañoso sobre bienes o recursos o intereses patrimoniales de naturaleza pública), representan un efecto económico.

  Ejemplo de efectos económicos que no son riesgos fiscales:

  i) Los riesgos de daño antijurídico, riesgo de pago de condenas y conciliaciones.

ii) Los efectos económicos generados por causas exógenas, es decir relacionadas con acción y omisión de los gestores públicos, como son hechos de fuerza mayor, caso fortuito o hecho de un tercero (es decir, de alguien que no tenga la calidad de gestor público).

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

- **Determinación del impacto o consecuencia en riesgos ambientales:**

Análisis Cualitativo: usa una escala de palabras o descripciones para examinar los impactos de cada evento que se origina y su posibilidad. Una matriz de riesgo con base en estas mediciones cualitativas (o declaradas) de las consecuencias y la eventualidad se puede usar como medio para combinar las consecuencias y las probabilidades de producir una medición del riesgo.

Tabla 24. Matriz para el análisis cualitativo del riesgo - nivel de riesgo

Posibilidad	Consecuencia				
	Catastrófica	Importante	Moderada	Menor	Insignificante
Casi seguro	E	E	E	A	A
Probable	E	E	A	A	M
Posible	E	E	A	M	A
Improbable	E	A	M	B	A
Raro	A	A	M	B	A
Convenciones: E = riesgo extremo, exige acción inmediata. A = riesgo alto, es necesaria la atención por parte de la alta dirección. M = riesgo moderado, se debe especificar la responsabilidad de la dirección. B = riesgo bajo, gestionado mediante procedimientos de rutina.					

Fuente: Gestión del riesgo ambiental principios y procesos – GTC 104

Análisis Semicuantitativo: a este análisis se le asigna valores de escalas cualitativas y después aplica una de varias fórmulas, para producir una clasificación de los riesgos. Este análisis no tiene como propósito producir estimados cuantitativos para el riesgo. El número adjudicado a cada descripción no tiene una relación precisa con la magnitud ni posibilidad real de las consecuencias, siempre y cuando el sistema usado para priorizar corresponda al sistema escogido para la asignación de los números y para su combinación.

Análisis Cuantitativo: usa valores numéricos tanto para las consecuencias como para la posibilidad. Los impactos se pueden estimar configurando los posibles resultados de un evento o conjunto de eventos o mediante la extrapolación de estudios experimentales o datos históricos. En algunos casos, se requiere más de un valor numérico para especificar las consecuencias para diferentes momentos, lugares, grupos o situaciones.

Determinación del Impacto o Consecuencia en Riesgos de Continuidad del Negocio: para calificar el impacto se utilizan los siguientes niveles (Tomado del Documento Continuidad de Negocio -Plan de Recuperación ante Desastres – DRP).

Tabla 25. Niveles de impacto

Niveles	Descripción Impacto (Consecuencias) Cuantitativo	Descripción Impacto (Consecuencias) Cualitativo
Insignificante	- Impacto que afecte la ejecución presupuestal, el cumplimiento de un programa o proyecto en un valor ≥0,5%. - Pérdida de cobertura en la prestación de los servicios de la Entidad ≥1%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la Entidad en un valor ≥0,5%. - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥0,5% del presupuesto general de la Entidad.	- No hay interrupción de las operaciones de la Entidad. - No se generan sanciones económicas o administrativas. - No se afecta la imagen institucional de forma significativa.
Menor	- Impacto que afecte la ejecución presupuestal, el cumplimiento de un programa o proyecto en un valor ≥1% - Pérdida de cobertura en la prestación de los servicios ≥5%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la Entidad en un valor ≥1%. - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥1% del presupuesto general de la Entidad.	- Interrupción de las operaciones de la Entidad por algunas horas. - Reclamaciones o quejas de los usuarios que implican investigaciones internas disciplinarias. - Imagen institucional afectada localmente por retrasos en la prestación del servicio a los usuarios o ciudadanos. - Heridas leves de personas, ya sean funcionarios, terceros trabajando en la Entidad o personal visitante.
Moderado	- Impacto que afecte la ejecución presupuestal, el cumplimiento de un programa o proyecto en un valor ≥5% - Pérdida de cobertura en la prestación de los servicios ≥10%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la Entidad en un valor ≥5%. - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥5% del presupuesto general de la Entidad.	- Interrupción de las operaciones de la Entidad por un (1) día. - Reclamaciones o quejas de los usuarios que podrían implicar una denuncia ante los entes reguladores o una demanda de largo alcance para la Entidad. - Inoportunidad en la información ocasionando retrasos en la atención a los usuarios.

Niveles	Descripción Impacto (Consecuencias) Cuantitativo	Descripción Impacto (Consecuencias) Cualitativo
		- Reproceso de actividades y aumento de carga operativa. - Imagen institucional afectada en el orden nacional o regional por retrasos en la prestación del servicio a los usuarios o ciudadanos. - Investigaciones penales, fiscales o disciplinarias. - Heridas graves de personas, ya sean funcionarios, terceros trabajando en la Entidad o personal visitante.
Mayor	- Impacto que afecte la ejecución presupuestal, el cumplimiento de un programa o proyecto en un valor ≥20%. - Pérdida de cobertura en la prestación de los servicios de la Entidad ≥20%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la Entidad en un valor ≥20%. - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥20% del presupuesto general de la Entidad.	- Interrupción de las operaciones de la Entidad por más de dos (2) días. - Pérdida de información crítica que puede ser recuperada de forma parcial o incompleta. - Sanción por parte del ente de control u otro ente regulador. - Incumplimiento en las metas y objetivos institucionales afectando el cumplimiento en las metas de gobierno. - Imagen institucional afectada en el orden nacional o regional por incumplimientos en la prestación del servicio a los usuarios o ciudadanos. - Reproceso de actividades y aumento de carga operativa. - Discapacidad o enfermedad permanente de personas, ya sean funcionarios, terceros trabajando en la Entidad o personal visitante.
Catastrófico	- Impacto que afecte la ejecución presupuestal de la Entidad, el cumplimiento a un programa o proyecto en un valor ≥50%. - Pérdida de cobertura en la prestación de los servicios ≥50%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el	- Interrupción de las operaciones de la Entidad por más de cinco (5) días. - Intervención por parte de un ente de control u otro ente regulador.

Niveles	Descripción Impacto (Consecuencias) Cuantitativo	Descripción Impacto (Consecuencias) Cualitativo
	presupuesto total de la Entidad en un valor ≥50%. - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥50% del presupuesto general de la Entidad.	- Pérdida de Información crítica para la Entidad que no se puede recuperar. - Incumplimiento en las metas y objetivos institucionales afectando de forma grave la ejecución presupuestal. - Imagen institucional afectada en el orden nacional o regional por actos o hechos de corrupción comprobados. - Reproceso de actividades y aumento de carga operativa: • Pérdida de vidas humanas por incidentes causados en las instalaciones de la Entidad.

Fuente: Continuidad de Negocio -Plan de Recuperación ante Desastres – DRP

Determinación del Impacto en Riesgos de Corrupción: 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.

Tabla 26. Criterios para calificar el impacto en riesgos de corrupción

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

Nivel de impacto MAYOR

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas - versión 6

- **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 6", bajo los mismos criterios establecidos para los riegos de gestión, asimilando 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.

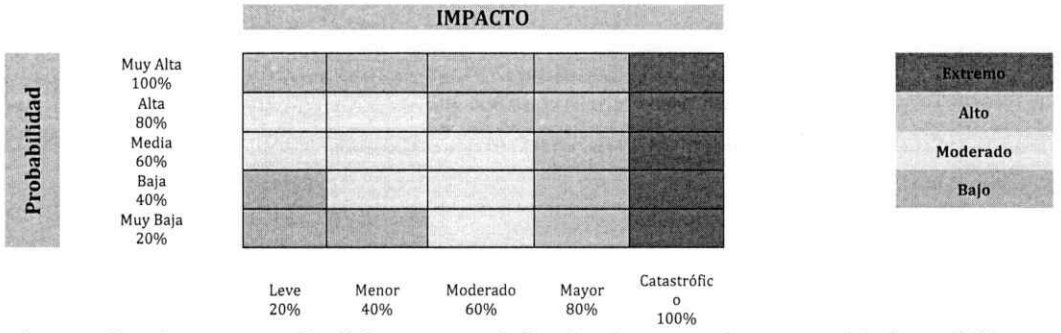
La probabilidad y el impacto se determinan con base en la amenaza y no en las vulnerabilidades.

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 (Seguridad y Salud en el Trabajo, Ambiental, Continuidad del Negocio, Conflicto de Intereses y Datos Personales): 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:

Tabla 27. Matriz valoración riesgo de gestión



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas - versión 6

Valoración del Riesgo Fiscal: a partir del análisis de la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto, se determina la zona de riesgo inicial (riesgo inherente), se define los niveles de severidad.

Ejemplo nivel de severidad riesgo fiscal:

Proceso: gestión de recursos

Objetivo: gestionar los bienes, obras y servicios administrativos, de mantenimiento y asistencia logística para el cumplimiento de la misión de la entidad.

Alcance: inicia con la consolidación y depuración del plan de necesidades de bienes, obras y servicios que requieran los procesos de la entidad en cada vigencia fiscal y culmina con el suministro de bienes y la prestación de los servicios, acorde con la disponibilidad de recursos.

Punto de Riesgo: ingreso, custodia y salida de bienes muebles de la entidad.

Riesgo Fiscal: posibilidad de efectos dañosos sobre bienes públicos (área de impacto), por pérdida, extravío o hurto de bienes muebles de la entidad (circunstancia inmediata), a causa de la omisión en la aplicación del procedimiento para el ingreso, custodia y salida de bienes e inventario del almacén y reporte de información a quien gestiona las pólizas cuando haya lugar (causa raíz).

Probabilidad: las veces que se pasa por el punto de riesgo en un año es 365, puesto que todos los días del año se debe ejercer la custodia de los bienes muebles de la entidad. Para el ejemplo es importante tener en cuenta que los bienes muebles en cada entidad varían en cantidad y son de distinto valor en el inventario, se sugiere analizar el tipo de bien y el número de estos, a fin de acotar el nivel de probabilidad con un análisis más ácido que permita establecer controles diferenciados acorde con la naturaleza de diferentes grupos de bienes (ejemplo: equipos de cómputo, muebles y enseres, entre otros).

Tabla 28. Ejemplo de valoración de riesgo fiscal

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

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

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas - versión 6

Es necesario cuantificar el potencial efecto dañoso sobre el bien, recurso o interés patrimonial de naturaleza pública para determinar el impacto. En el ejemplo el efecto dañoso sería del valor contable del inventario de bienes muebles que para el ejemplo se determina que es de $2.500 millones de pesos, lo cual corresponde a 2.500 SMLMV, de acuerdo a la matriz del nivel de impacto sería catastrófico.

Tabla 29. Ejemplo de afectación económica con impacto catastrófico del riesgo fiscal

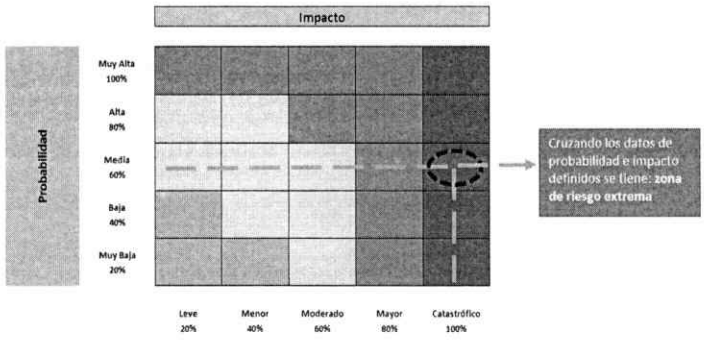
	Afectación Económica	Reputacional
Leve 20%	Afectación menor a 10 SMLMV	El riesgo afecta la imagen de algún área de la entidad.
Menor 40%	Entre 10 y 50 SMLMV	El riesgo afecta la imagen de la entidad internamente de conocimiento general nivel interno, de junta directiva y/o de proveedores.
Moderado 60%	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.
Catastrófico 100%	Mayor a 500 SMLMV	El riesgo afecta la imagen de la entidad nacional, con efecto publicitario sostenido a nivel país.

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas - versión 6

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

Zona de severidad o nivel de riesgo: al realizar la valoración de la probabilidad con el impacto, el resultado da un riesgo extremo.

Ilustración 10. Matriz de valoración del riesgo fiscal



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas - versión 6

Valoración Riesgo en Seguridad y Salud en el Trabajo: la valoración de los riesgos es la base para la gestión proactiva de la seguridad y salud en el trabajo, liderada por la Alta Dirección como parte de la gestión integral del riesgo, con la participación y compromiso de todos los niveles de la entidad y otras partes interesadas. Independientemente de la complejidad de la valoración de los riesgos, ésta debería ser un proceso sistemático que garantice el cumplimiento de los propósitos.

Todos los empleados tendrían que identificar y comunicar a su empleador los peligros asociados a su actividad laboral. Los empleadores tienen el deber de evaluar los riesgos derivados de estas actividades laborales.

El procedimiento de valoración de riesgos que se describe en esta guía está destinado a ser utilizado en:

- Situaciones en que los peligros puedan afectar la seguridad o la salud y no haya certeza de que los controles existentes o planificados sean adecuados, en principio o en la práctica;
- Organizaciones que buscan la mejora continua de seguridad y salud en el trabajo y el cumplimiento de los requisitos legales;
- Situaciones previas a la implementación de cambios en sus procesos e instalaciones.

Aspectos a Tener en Cuenta para Desarrollar la valoración de los Riesgos:

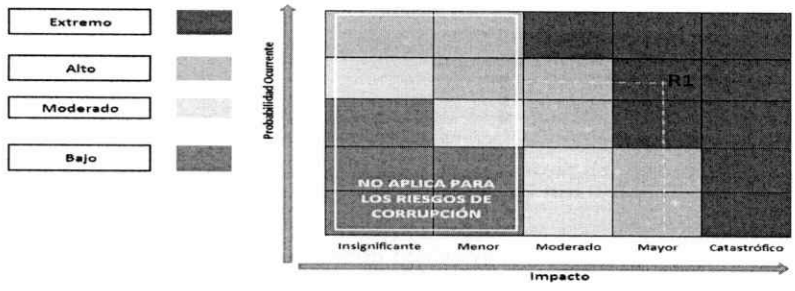
Valorar Riesgo:

- Evaluar el Riesgo: calificar el riesgo asociado a cada peligro, incluyendo los controles existentes que están implementados. Se debería considerar la eficacia de dichos controles, así como la probabilidad y las consecuencias si éstos fallan.
- Definir los criterios para determinar la aceptabilidad del riesgo.
- Definir si el riesgo es aceptable: determinar la aceptabilidad de los riesgos y decidir si los controles de seguridad y salud en el trabajo existente o planificado son suficientes para mantener los riesgos bajo control y cumplir los requisitos legales.

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 y 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 6, 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:

Tabla 30. Matriz valoración riesgo de corrupción



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas - Versión 6

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

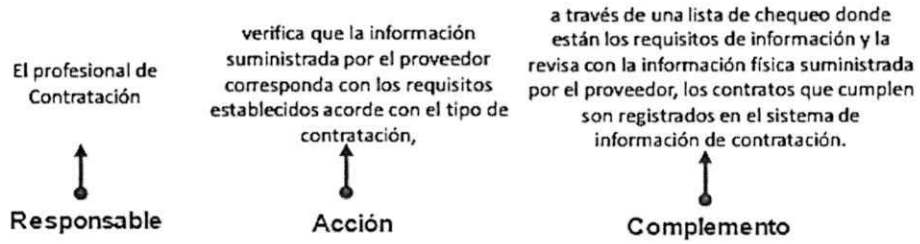
Valoración de Controles en Riesgos de Gestión (Seguridad y Salud en el Trabajo, Ambiental, Conflicto de Intereses, Continuidad del Negocio, y Datos Personales): conceptualmente un control se define como la medida que permite reducir o mitigar el riesgo, el cual se debe tener en cuenta:

- 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.

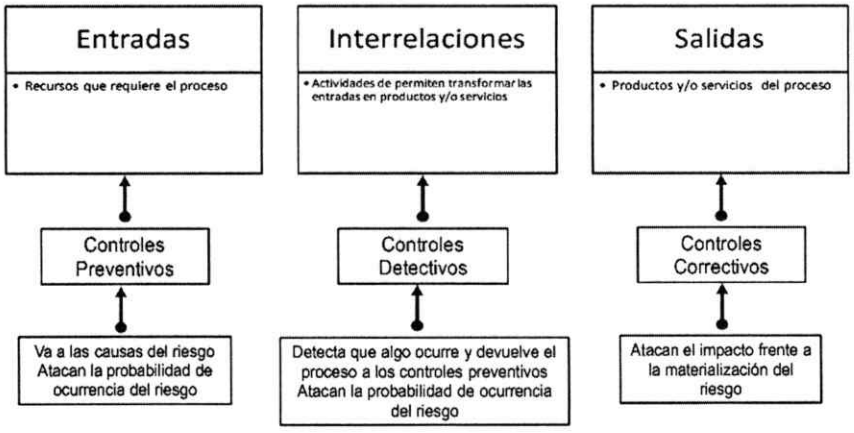
Ilustración 11. Ejemplo. Estructura para la redacción del control



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas - Versión 6

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:

Ilustración 12. Tipología de controles y los procesos



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas - versión 6

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:

Tabla 31. Atributos para el diseño de control

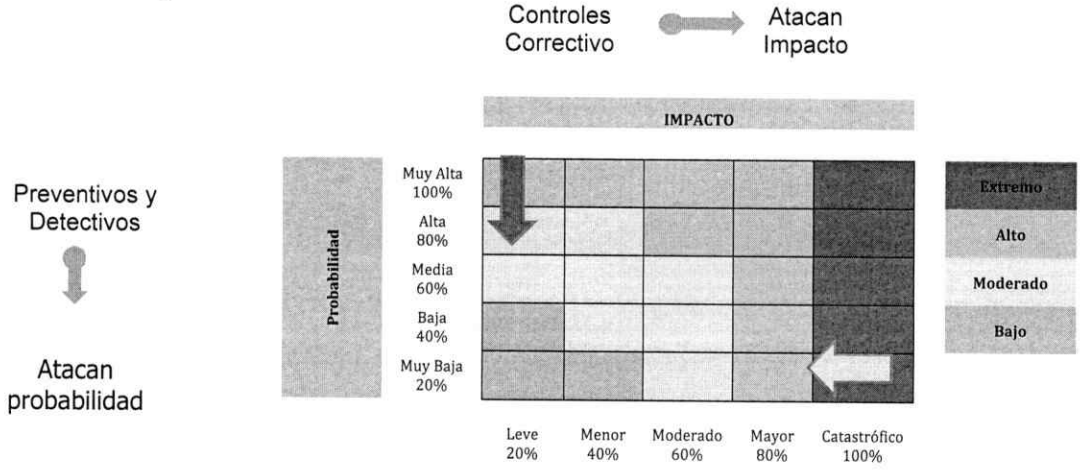
Características			Descripción	Peso
Atributos de eficiencia	Tipo	Preventivo	Va hacia las causas del riesgo, aseguran el resultado final esperado.	25%
		Detectivo	Detecta que algo ocurre y devuelve el proceso a los controles preventivos. Se pueden generar reprocesos.	15%
		Correctivo	Dado que permiten reducir el impacto de la materialización del riesgo, tienen un costo en su implementación.	10%
	Implementación	Automático	Son actividades de procesamiento o validación de información que se ejecutan por un sistema y/o aplicativo de manera automática sin la intervención de personas para su realización.	25%
		Manual	Controles que son ejecutados por una persona, tiene implícito el error humano.	15%
*Atributos 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.	-

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas - Versión -6

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

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

Tabla 32. Tipos de controles



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas - versión 6

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 usará con el valor resultante luego de la práctica 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 Riesgo Fiscal: las actividades de control, se orientan a prevenir y detectar la materialización de los riesgos.

Tipologías de controles:

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

Para el análisis y evaluación de los controles se analizan los atributos para el diseño del control, teniendo en cuenta características relacionadas con la eficiencia y la formación (Se aplican los lineamientos para la redacción del control establecidas en la "Estructura para la Redacción del Control" y definidas en "Análisis y evaluación de los controles – atributos".

Ejemplo:

Proceso: gestión de recursos

Objetivo: gestionar los bienes, obras y servicios administrativos, de mantenimiento y asistencia logística para el cumplimiento de la misión de la entidad.

Alcance: inicia con la consolidación y depuración del plan de necesidades de bienes, obras y servicios que requieran los procesos institucionales en cada vigencia fiscal y culmina con el suministro de bienes y la prestación de los servicios, acorde con la disponibilidad de recursos.

Punto de Riesgo: ingreso, custodia y salida de bienes muebles de la entidad.

Riesgo Fiscal: posibilidad de efectos dañoso sobre bienes públicos (área de impacto), por pérdida, extravío o hurto de bienes muebles de la entidad (circunstancia inmediata), a causa de la omisión en la aplicación del procedimiento para el ingreso, custodia y salida de bienes e inventario del almacén y el reporte de información a que gestiona las pólizas cuando haya lugar (causa raíz).

Probabilidad Inherente: Media 60%
Impacto Inherente: Catastrófico 100%
Zona de Riesgo: Extrema establecer condiciones

Ejemplo de Controles Identificados:

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

Tabla 33. Valoración de controles en el riesgo fiscal

Control 1	Criterios de Efectividad			Peso
El jefe de almacén valida y registra diariamente las entradas y salidas en el aplicativo dispuesto para tal fin, el cual alimenta automáticamente el inventario de bienes muebles de la entidad y su responsable.	Tipo	Preventivo	X	25%
		Detectivo		
		Correctivo		
	Implementación	Automático		
		Manual	X	15%

	Total, Valoración Control 1_=40%			
Control 2	**Criterios de Efectividad**			**Peso**
El coordinador administrativo verifica mensualmente la relación de ingreso y salida de bienes muebles contra los inventarios generados por el sistema (actualización y ubicación en el inventario), en caso de encontrar inconsistencias solicita al jefe de almacén ubicar el bien faltante y realizar el ajuste, teniendo en cuenta los soportes de salida e ingreso del almacén.	Tipo	Preventivo		
		Detectivo	X	15%
		Correctivo		
	Implementación	Automático		
		Manual	X	15%
	Total, Valoración Control 2=30%			
Control 3	**Criterios de Efectividad**			**Peso**
El director administrativo verifica la vigencia y actualización de la póliza de acuerdo a los bienes que ingresan a la entidad, en caso de presentarse un siniestro adelanta las reclamaciones respectivas ante el asegurador.	Tipo	Preventivo		
		Detectivo		
		Correctivo	X	10%
	Implementación	Automático		
		Manual	X	15%
	Total, Valoración Control 3=25%			

Nivel de Riesgo (Riesgo Residual)

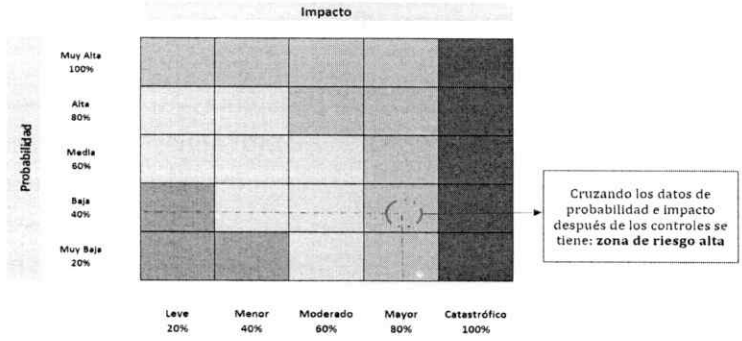
Para la aplicación de los controles se debe tener en cuenta que estos mitigan el riesgo de forma acumulativa, esto quiere decir que una vez se aplica el calor de uno de los controles, el siguiente control se aplicará con el valor resultante luego de la aplicación del primer control.

Tabla 34. Ejemplo para la aplicación de los controles

Riesgo	Datos Relacionados con la probabilidad e Impacto Inherentes		Datos Valoración de Controles		Cálculos Requeridos
Posibilidad de efectos dañoso sobre bienes públicos (área de impacto), por pérdida, extravío o hurto de bienes muebles de la entidad (circunstancia inmediata), a causa de la omisión de cumplimiento del procedimiento para el ingreso, custodia y salida de bienes e inventario del almacén y el reporte de información a quien gestiona las pólizas cuando haya lugar (causa raíz).	Probabilidad Inherente	60%	Valoración Control 1 Preventivo	40%	60%*40%=24% 60%-24%=36%
	Valor Probabilidad para Aplicar 2º Control	36%	Valoración Control 2 Dectectivo	30%	36%*30%=10.8% 36%-10,8%=25,2%
	Probabilidad Residual	25,2%			
	Impacto Inherente	100%	Valoración Control Correctivo	25%	100%*25%=25% 100%-25%=75%
	Impacto Residual	75%			

En la matriz de calor se muestra cuál es el movimiento en el eje de probabilidad y en el eje de impacto de acuerdo con los tipos de controles y cálculo final:

Ilustración 13. Matriz de calor de acuerdo a los tipos de controles



Valoración de Controles en los Riesgos de Continuidad del Negocio: la valoración de los controles parte de realizar la identificación de aquellos que tengan influencia directa, en la mitigación del impacto o la reducción de la probabilidad del riesgo.

Para los riesgos de seguridad de la información, se considera los siguientes criterios de valoración de controles. Para los otros riesgos evaluados por la Entidad, los criterios de valoración se encuentran en el "FORMATO PARA LA DEFINICIÓN, VALORACIÓN, ANÁLISIS Y EVALUACIÓN DE CONTROLES ".

Tabla 35. Criterios de valoración

Criterios para la evaluación	Evaluación		Observaciones
	Sí	No	
¿El control previene la materialización del riesgo (afecta probabilidad)? ¿El control permite enfrentar la situación en caso de materialización (afecta impacto)?			Este criterio no puntúa, es relevante determinar si el control es preventivo (probabilidad) o si es correctivo que permite enfrentar el evento una vez materializado (impacto), con el fin de establecer el desplazamiento en la matriz de evaluación de riesgos.
¿El control cuenta con una descripción que indique claramente que hace y si su propósito es adecuado para el riesgo?	15	0	Una adecuada descripción del control debe considerar una estructura como: Qué, Cómo, Para qué y Cuándo. Ejemplos: -Definir lineamientos de atención al ciudadano, adoptando políticas internas para mejorar la prestación de los servicios. -Implementar un sistema de información, definiendo controles automatizados, que genere alertas de vencimientos de términos e informes en tiempo real sobre el estado actual de las solicitudes realizadas por los ciudadanos.
¿Está(n) definido(s) el(los) responsable(s) de la ejecución del control y del seguimiento?	5	0	

Criterios para la evaluación	Evaluación		Observaciones
	Sí	No	
¿La frecuencia de ejecución del control y seguimiento es indicada y es adecuada?	15	0	
¿El control es automático?	15	0	Sistemas o Software que permiten incluir contraseñas de acceso, o con controles de seguimiento a aprobaciones o ejecuciones que se realizan a través de éste, generación de reportes o indicadores, sistemas de seguridad con scanner, sistemas de grabación, entre otros.
¿En el tiempo que lleva la herramienta ha demostrado ser efectiva?	15	0	Si es automático.
¿El control es manual?	10	0	Políticas de operación aplicables, autorizaciones a través de firmas o confirmaciones vía correo electrónico, archivos físicos, consecutivos, listas de chequeo, controles de seguridad con personal especializado, entre otros.
¿El control está documentado formalmente?	15	0	La documentación formal del control permite determinar que el control se ejecute con los mismos atributos a lo largo del tiempo.
¿Se cuenta con evidencias de la ejecución y seguimiento del control acorde a las definiciones de los criterios anteriores?	10	0	

Fuente: Continuidad de negocio -Plan de Recuperación ante Desastres – DRP- UIAF

Estimar el Nivel de Riesgo Residual: de acuerdo con lo establecido en la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas del Departamento Administrativo de la Función Pública -DAFP, la valoración del riesgo 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).

Para identificar el nivel de probabilidad e impacto residual considerando si el control afecta la probabilidad o impacto (primer criterio de evaluación de controles presentado) se consideran los siguientes criterios para desplazar en la matriz de evaluación de riesgos:

Tabla 36. Criterios para desplazar en la matriz de evaluación de riesgos

Solidez	Descripción
Fuerte	El promedio de la solidez individual de cada control al sumarlos y ponderarlos es igual a 100.
Moderado	El promedio de la solidez individual de cada control al sumarlos y ponderarlos está entre 50 y 99.
Débil	El promedio de la solidez individual de cada control al sumarlos y ponderarlos es menor a 50.

Fuente: Continuidad de negocio -Plan de Recuperación ante Desastres – DRP- UIAF

Tabla 37. Matriz de controles para la identificación del riesgo

Solidez del Conjunto de los Controles	Controles Ayudan a Disminuir la Probabilidad	Controles Ayudan a Disminuir el Impacto	# de Columnas en la Matriz de Riesgo que se Desplaza en el Eje de la Probabilidad	# de Columnas en la Matriz de Riesgo que se Desplaza en el Eje del Impacto
Fuerte	Directamente	Directamente	2	2
Fuerte	Directamente	Indirectamente	2	1
Fuerte	Directamente	No Disminuye	2	0
Fuerte	No Disminuye	Directamente	0	2
Moderado	Directamente	Indirectamente	1	1
Moderado	Directamente	No Disminuye	1	0
Moderado	Directamente	Directamente	1	0
Moderado	No Disminuye	Indirectamente	0	1
Débil	No Disminuye	No Disminuye	0	0

Fuente: Continuidad de negocio -Plan de Recuperación ante Desastres – DRP- UIAF

Una vez analizados los controles para el riesgo identificado y determinado el número de niveles a mover en la matriz de evaluación del riesgo, se establece el riesgo residual.

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 6", 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 digital empleando como mínimo los controles del Anexo A de la norma técnica ISO/IEC 27001:2013, estos controles se encuentran en el "**Anexo 4. Lineamientos para la gestión de riesgos de seguridad digital 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.

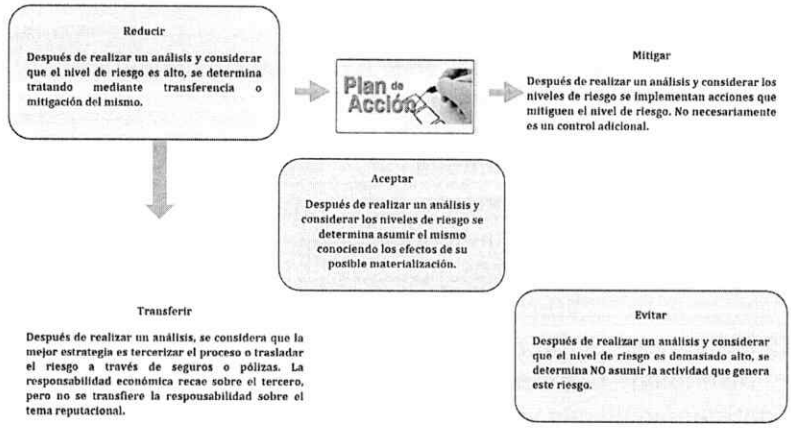
7.4 Estrategias para Combatir el Riesgo

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.

Ilustración 14. Estrategias para combatir el riesgo



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas - versión 6

7.5. Monitoreo y Revisión

El Modelo Integrado de Planeación y Gestión (MIPG) desarrolla a través de la dimensión 7, el Control Interno y 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, trimestralmente los líderes de proceso con el apoyo y acompañamiento de la Oficina Asesora de Planeación y de la Oficina de Control Interno e Inspección, identifican y/o validan los riesgos de gestión (seguridad y salud en el trabajo, ambiental, continuidad de negocio, conflicto de intereses y datos personales), fiscal, seguridad digital y corrupción, 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 posteriormente por las auditorías internas, programadas por la Oficina de Control Interno e Inspección.

El monitoreo a los riesgos de gestión (seguridad y salud en el trabajo, ambiental, continuidad de negocio, conflicto de intereses y datos personales), fiscal, seguridad digital, deberá realizarse trimestralmente, con

corte a marzo 31, a junio 30, septiembre 30 y a diciembre 31, y los de corrupción mensualmente. 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 que 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 e Inspección (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.

7.6. Niveles de Aceptación del Riesgo

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

Tabla 38. Niveles de aceptación

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.

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas- versión 6

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, por tal razón, 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.

7.6.1. Niveles de Aceptación para los Riesgos de Gestión (Seguridad y Salud en el Trabajo, Ambiental, Conflicto de Intereses y Datos Personales)

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.**

7.6.2. Niveles de Aceptación para los Riesgos Fiscal

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

7.6.3. 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.

7.6.4. Niveles de Aceptación para los Riesgos de Continuidad del Negocio

a. **Zona de Riesgo Baja:** la tolerancia al riesgo en la Entidad considera la zona de riesgo baja. Se realizarán seguimientos **TRIMESTRAL** por parte de los líderes de los procesos para evitar a toda costa su materialización.
b. **Zona de Riesgo Moderada:** los riesgos que se ubiquen en esta zona, pueden asumirse y (ser tolerables), o se les puede aplicar un plan de tratamiento que permita reducir su probabilidad o impacto. Se realizarán seguimientos **TRIMESTRAL** por parte de los líderes de los procesos, para evitar a toda costa su materialización.
8. **Zona de Riesgo Alta y Zona de Riesgo Extrema:** para los riesgos residuales que se encuentren aún fuera de la zona de tolerancia de riesgo definida por la Entidad, es necesario que los líderes de procesos establezcan planes de tratamiento considerando las opciones de reducir, transferir o evitar. Se realizan seguimientos **MENSUALES** por parte de los líderes de los procesos, para evitar a toda costa su materialización.

9. HISTORIAL 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".	20 de diciembre de 2021
4	Actualización con base en la versión 4 del mapa de procesos de la entidad	Se cambia el nombre del proceso y el código correspondiente del SIG debido a la modificación del mapa de procesos, pasando del SIG-PO-01 al DPE-PO-01; Se cambia la versión de la política; Se actualiza la introducción del presente documento; Se actualiza el marco normativo, eliminado las normas que perdieron vigencia e incorporando la nueva normatividad aplicable; Se adicionan nuevos términos al capítulo 4; Se actualiza el capítulo 7.4. de acuerdo con la versión vigente del plan estratégico Institucional y la plataforma estratégica de la entidad; Se actualiza el capítulo 7.5 con la versión 4 del mapa de procesos; Se integra dentro de la política de administración del riesgo, los riesgos de seguridad y salud en el trabajo, ambiental, continuidad del negocio, conflicto de intereses y datos personales.	25 de agosto de 2022
5	Se actualiza con base en el nuevo Plan Estratégico Institucional 2023-2026, Revisión y actualización de la	Se actualiza la imagen de la portada del documento; Se ajusta la introducción y objetivo; En el marco normativo se adicionan: Ley: 526 de 1999,610 de 2000,1121 de 2006, 1437 de 2011, 1581 e 2012, 1621 de 2013,1712 de 2014, 1952 de 2019, Decreto: 1377 de 2013, 857 de 2014,	05 de junio de 2024

	política de acuerdo a la versión 6 de la guía para la administración del riesgo y el diseño de controles en entidades públicas.	403 e 2020, 153 de 2022, Resolución 33 de 2023, Guía para la identificación de los peligros y la valoración de los riesgos de seguridad y salud ocupacional -GTC 45 de 2012; Acto Legislativo 04 de 2019; Se ajusta el ítem de roles y responsabilidades frente al riesgo en las líneas de defensa; Se elimina el ítem tipo de política al estar contenido en la metodología. Se actualizan los ítems correspondientes a la alineación de la política de administración del riesgo con la plataforma estratégica de la entidad: propósito superior, misión, visión, líneas de acción y estrategias; Se adiciona el riesgo fiscal de acuerdo a los lineamientos del 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 6 de noviembre de 2022.	