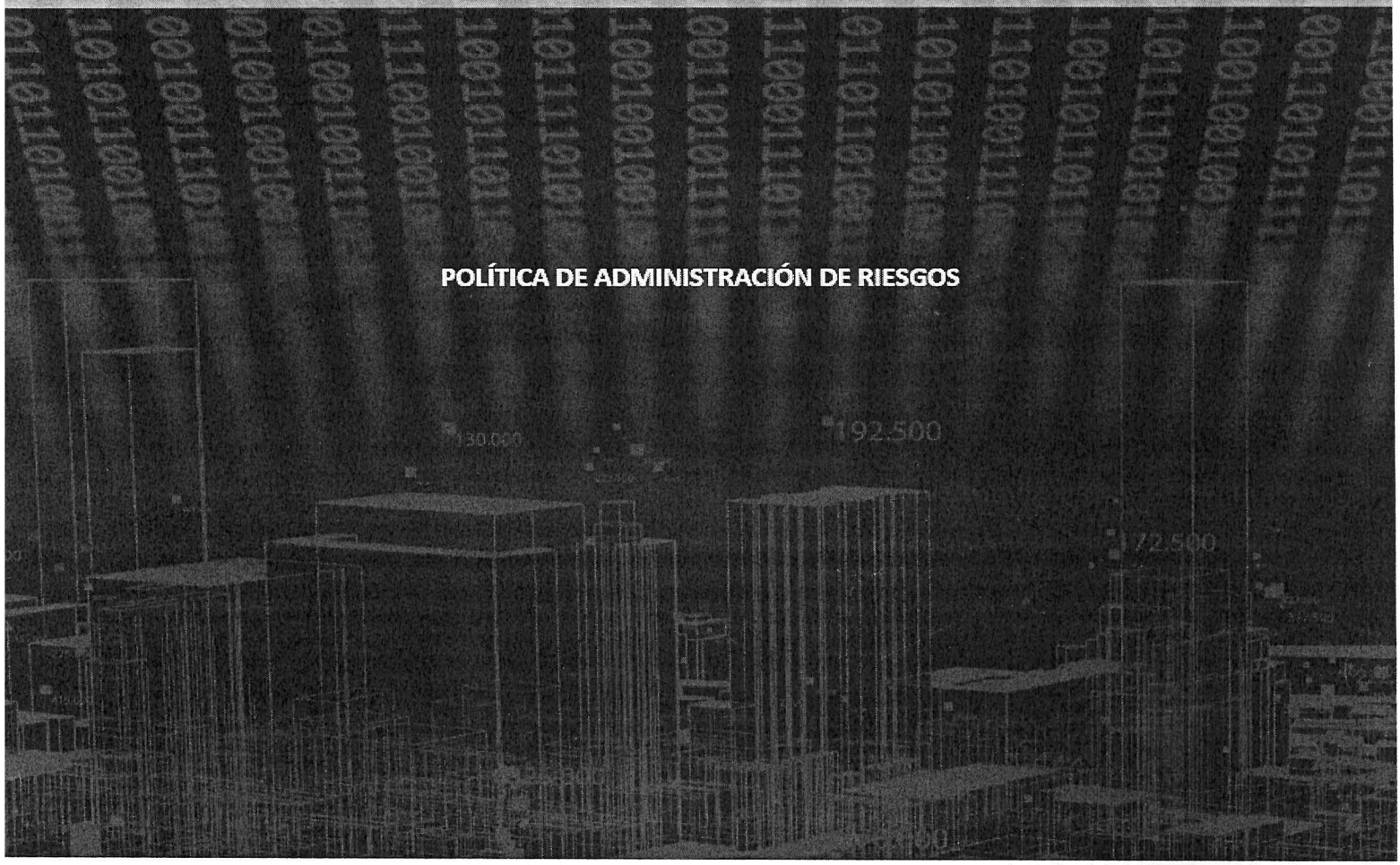
MINISTERIO DE HACIENDA Y CRÉDITO PÚBLICO



POLÍTICA DE ADMINISTRACIÓN DE RIESGOS

	PREPARÓ	REVISÓ	APROBÓ
FIRMA:			
CÓDIGO:	302	93, 241,306, 266, 226 108, 131,21, 54, 165	100
CARGO:	Profesional Especializado OAP	Subdirectora SAO, Subdirector SAE (E), Subdirección de Analítica (E), subdirector STI, Subdirector SAF, Jefe OAJ, Jefe Oficina Asuntos Internacionales, Jefe OCI, Jefe Oficina Asesora de Planeación, Profesional Especializado OAP	Director General
FECHA:	8 de agosto de 2022	19 de agosto de 2022	25 de agosto de 2022

Lista de Ilustraciones

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

1. Objetivo

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

2. Alcance

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

3. Marco Normativo

- Constitución Política de Colombia de 1991, a través de la cual se adopta los principios de la función administrativa y elimina el control fiscal previo y obligatoriedad para todas las entidades estatales de contar con el control interno;
- Literal a) del Artículo 2° de la Ley 87 de 1993 – Objetivos del Control Interno. Proteger los recursos de la organización, buscando su adecuada administración ante posibles riesgos que los afectan;
- Literal f) del Artículo 2° de la Ley 87 de 1993 – Objetivos del Control Interno. Definir y aplicar medidas para prevenir los riesgos, detectar y corregir las desviaciones que se presenten en la organización y que puedan afectar el logro de los objetivos;
- Ley 1562 de 2012" Por la cual se modifica el sistema de riesgos laborales y se dictan otras disposiciones en materia de salud ocupacional";
- Ley 489 de 1998, a través de la cual se fortalece el Control Interno, mediante la creación del Sistema Nacional de Control Interno;
- Ley 2195 de 2022 "Por medio de la cual se adoptan medidas en materia de transparencia, prevención y lucha contra la corrupción y se dictan otras disposiciones"
- Decreto 1072 de 2015 "Por el cual se dictan disposiciones para la implementación del Sistema de Gestión de la Seguridad y Salud en el Trabajo (SG-SST).";

- **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 (Tomado 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.
- **Administración de Riesgos**: proceso efectuado por la Alta Dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos. El enfoque de riesgos no se determina solamente con el uso de la metodología, sino logrando que la evaluación de los riesgos se convierta en una parte natural del proceso de planeación.
- **Alta Dirección:** persona o grupo de personas del máximo nivel jerárquico que dirigen y controlan una entidad.
- **Amenaza:** medida que modifica el riesgo (procesos, políticas, dispositivos, prácticas u otras acciones).
- **Análisis de Riesgo:** elemento de control que permite establecer la probabilidad de ocurrencia de los eventos positivos y/o negativos y el impacto de sus consecuencias, calificándolos y evaluándolos a fin de determinar la capacidad de la entidad pública para su aceptación y manejo. Se debe llevar a cabo un uso sistemático de la información disponible para determinar qué tan frecuentemente pueden ocurrir eventos especificados y la magnitud de sus consecuencias.
- **Apetito del Riesgo:** es el nivel de riesgo que la entidad puede aceptar, relacionado con sus objetivos, el marco legal y las disposiciones de la Alta Dirección y del Órgano de Gobierno. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar (Tomado de la guía para la administración del Riesgo y el diseño de controles en entidades públicas - versión 5).
- **Autoevaluación del Control:** elemento de control que, basado en un conjunto de mecanismos de verificación y evaluación, determina la calidad y efectividad de los controles internos a nivel de los procesos y de cada área organizacional responsable, permitiendo emprender las acciones de mejoramiento del control requeridas. Se basa en una revisión periódica y sistemática de los procesos de la entidad para asegurar que los controles establecidos son aún eficaces y apropiados.
- **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 (Tomado de la Norma Internacional ISO 19011).
- **Auditoría conjunta:** auditoría llevada a cabo a un único auditado por dos o más organizaciones auditoras. (Tomado de la Norma Internacional ISO 19011)
- **Auditoria de Gestión:** es una evaluación que se le realiza a una entidad para establecer el grado de eficiencia, eficacia en la planeación, control y uso de los recursos (Tomado de la Norma Internacional ISO 19011).
- **Auditoria de Requisitos:** es una verificación del cumplimiento de los requisitos mínimos necesarios para implementar un sistema de gestión de calidad. Las entidades necesitan demostrar su capacidad para proporcionar regularmente productos y servicios que cumplen con los requisitos del cliente y los legales y reglamentarios aplicables y que aspiran aumentar la satisfacción del cliente.

- **Contingencia:** acción que debe seguirse al momento de materializarse el riesgo, con el fin de seguir prestando el servicio o se puedan desarrollar las operaciones con el menor traumatismo posible.
- **Control:** medida que permite reducir o mitigar un riesgo (Tomado de la guía para la administración del Riesgo y el diseño de controles en entidades públicas - versión 5).
- **Control adecuado:** es el que está presente si la dirección ha planificado y organizado (diseñado) las operaciones de manera tal que proporcionen un aseguramiento razonable de que los objetivos y metas de la organización serán alcanzados de forma eficiente y económica.
- **Corrupción:** uso del poder para desviar la gestión de lo público hacia el beneficio privado.
- **Criterios de auditoria:** conjunto de políticas, procedimientos o requisitos usados como referencia frente a la cual se compara la evidencia de la auditoria (Tomado de la Norma Internacional ISO 19011).
- **Dato personal:** cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables (Tomado de la Ley estatutaria 1581 de 2012).
- **Disponibilidad:** propiedad de ser accesible y utilizable a demanda por una entidad (Tomado de la guía para la administración del Riesgo y el diseño de controles en entidades públicas - versión 5).
- **Eficacia:** grado en el que se realizan las actividades planificadas y se logran los resultados planificados.
- **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 (Tomado de la Ley estatutaria 1581 de 2012).
- **Evaluación del Riesgo:** proceso utilizado para determinar las prioridades de la Administración del Riesgo comparando el nivel de un determinado riesgo con respecto a un estándar determinado.
- **Evidencia de la auditoria:** registros, declaraciones de hechos o cualquier otra información que es pertinente para los criterios de la auditoria y es verificable (Tomado de la Norma Internacional ISO 19011).
- **Factores de Riesgo:** son las fuentes generadoras de riesgos (Tomado de la guía para la administración del Riesgo y el diseño de controles en entidades públicas - versión 5).
- **Gestión del Riesgo de Corrupción:** proceso para identificar, evaluar, manejar y controlar acontecimientos o situaciones potenciales, con el fin de proporcionar un aseguramiento razonable respecto al alcance de los objetivos de la organización.
- **Identificación del peligro:** proceso para reconocer si existe un peligro y definir sus características. (Tomado de la guía para la identificación de los peligros y la valoración de los riesgos de seguridad y salud ocupacional -GTC 45 -segunda actualización).
- **Identificación del Riesgo:** elemento de control, que posibilita conocer los eventos potenciales, estén o no bajo el control de la entidad pública, que ponen en riesgo el logro de su misión, estableciendo los agentes generadores, las causas y los efectos de su ocurrencia. se puede entender como el proceso que permite determinar qué podría suceder, por qué sucedería y de qué manera se llevaría a cabo.

de veces que se pasa por el punto de riesgo en el periodo de 1 año (Tomado de la guía para la administración del Riesgo y el diseño de controles en entidades públicas - versión 5).

- **Proceso:** conjunto de actividades mutuamente relacionadas o que interactúan para generar un valor.
- **Programa de auditoría:** acuerdos para un conjunto de una o más auditorías planificadas para un periodo de tiempo determinado y dirigidas hacia un propósito específico.
- **Reporte de Materialización de Riesgos:** adicionalmente al monitoreo de los riesgos, que los responsables de cada proceso deben realizar periódicamente a su mapa de riesgos, cualquier funcionario o contratista que conozca de la materialización de un riesgo debe reportarlo a la Oficina Asesora de Planeación a través del instrumento o canal que ésta defina.
- **Requisito:** necesidad o expectativa establecida, generalmente implícita u obligatoria (Tomado de la Norma Internacional ISO 19011).
- **Riesgo:** efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales. Los eventos potenciales hacen referencia a la posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos (Tomado de la guía para la administración del Riesgo y el diseño de controles en entidades públicas - versión 5).
- **Riesgo Aceptable:** riesgo que ha sido reducido a un nivel que la organización puede tolerar con respecto a sus obligaciones legal (Tomado de la guía para la identificación de los peligros y la valoración de los riesgos de seguridad y salud ocupacional -GTC 45 -segunda actualización).
- **Riesgo de Corrupción:** posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado (Tomado de la guía para la administración del Riesgo y el diseño de controles en entidades públicas - versión 5).
- **Riesgo de Gestión:** posibilidad de que suceda algún evento que tendrá un impacto sobre el cumplimiento de los objetivos. Se expresa en términos de probabilidad y consecuencias.
- **Riesgos de las Auditorias:** se refiere tanto a los riesgos del proceso de auditoria para alcanzar sus objetivos, como al riesgo potencial de la auditoria para interferir con las actividades y procesos del auditado (Tomado de la Norma Internacional ISO 19011).
- **Riesgo de Conflicto de Intereses:** cuando el interés general propio de la función pública entra en conflicto con el interés particular y directo del servidor público (Tomado de Guía para la identificación y declaración del conflicto de intereses en el sector público colombiano - versión 2).
- **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. Amenazas y vulnerabilidades que pueden comprometer la disponibilidad de funciones de negocio, que dan soporte a los procesos de la UIAF
- **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).

Tabla 1 Roles y Responsabilidades de Acuerdo con las Líneas de Defensa

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

Líneas de Defensa	Responsables	Roles y Responsabilidades
		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.

Líneas de Defensa	Responsables	Roles y Responsabilidades
Segunda Línea de Defensa Asegura que los controles y los procesos de gestión de riesgos implementados por la primera Línea de Defensa, estén diseñados apropiadamente y funcionen como se pretende	**Jefes de Planeación,** **Supervisores e Interventores de Contratos o Proyectos,** **Coordinadores de Otros Sistemas de Gestión de la Entidad,** **Comités de Riesgos (donde existan),** **Comités de Contratación** **Área financiera, TIC, seguridad de la información, PQRSD y demás que provean aseguramiento a la tercera Línea de Defensa**	**a. Roles y Responsabilidades** 1. Monitorear la gestión de riesgo y control ejecutada por la Primera Línea de Defensa, complementando su trabajo; 2. Asegurar que los controles y procesos de gestión de riesgos implementados por la Primera Línea de Defensa, estén diseñados apropiadamente y funcionen como se pretende. **b. Actividades a Realizar** 1. La Oficina Asesora de Planeación o quien haga sus veces, define la metodología para la administración del riesgo, acorde a la normatividad y lineamientos para cada tipo de riesgo a excepción de los riesgos que por naturaleza requieran una metodología particular (Riesgos ambientales, de seguridad 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 y el entorno y cómo esos pueden generar nuevos riesgos o modificar los que ya se

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

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

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

6.2.3. Visión

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

6.2.4. 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 con el fin de que los actores del Sistema ALA/CFT adopten mecanismos, instrumentos y medidas, que se ajusten a la normatividad nacional e internacional.

Estrategia 1.1. Fortalecer el conocimiento y la cultura antilavado en todos los actores del Sistema ALA/CFT.
Estrategia 1.2. Crear tanques de pensamiento para fortalecer el entendimiento de temas relacionados con LA/FT.
Estrategia 1.3. Implementar la Evaluación Nacional del Riesgo (ENR) Digital para una identificación más oportuna del riesgo frente al LA/FT.
Estrategia 1.4. Implementar política pública tendiente a robustecer el funcionamiento del Sistema ALA/CFT del país.

b) Línea de Acción 2. - Detección

Objetivo Estratégico: detectar e identificar las redes criminales de LA/FT nacionales y transnacionales a través del entendimiento de las dinámicas de la amenaza y del análisis financiero.

Estrategia 2.1. Activar la metodología G4 (Minería de Datos, Redes Complejas, Análisis Macrosectorial y Análisis Financiero).
Estrategia 2.2. Fortalecer el trabajo conjunto con la FGN, cooperar con organismos de inteligencia nacionales y demás actores del Sistema ALA/CFT y adelantar actividades coordinadas con homólogos u organismos internacionales de similar naturaleza.
Estrategia 2.3. Actualizar de manera permanente las fuentes de información.
Estrategia 2.4. Detectar estructuras de Lavado Sofisticado a partir de la Metodología G4.

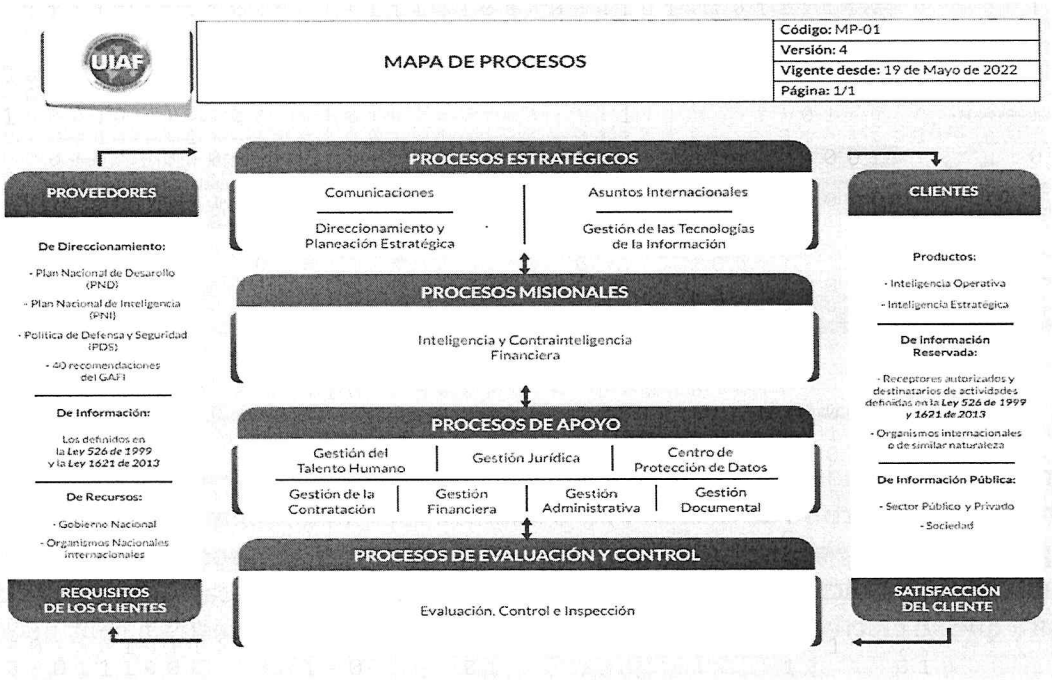
C) Línea de Acción 3. - Transformación tecnológica e innovación

Objetivo Estratégico: implementar proyectos de modernización tecnológica que soporten el desarrollo del Sistema Dinámico y Efectivo (SDE), apalancándose en herramientas innovadoras.

Estrategia 3.1. Dinamizar el acceso a la información requerida por la entidad.

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 5, diciembre de 2020. De igual manera, se incorporan los lineamientos definidos en el Modelo Integrado de Planeación y Gestión – MIPG, la Guía para la identificación y declaración del conflicto de intereses en el Sector Público colombiano, emitida por el DAFP.

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

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 en los próximos cuatro años. Este Marco Estratégico, parte de un análisis de contexto que permite conocer en dónde se encuentra la entidad y cuál será su direccionamiento para el siguiente periodo de gobierno.

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

Tabla 3 Contexto

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

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

Establecer el contexto define los parámetros básicos dentro de los cuales se deben gestionar los riesgos y establece el alcance para el resto del proceso de gestión del riesgo. El contexto incluye al ambiente interno y externo de la organización y el propósito de la actividad de gestión de riesgo. También incluye la consideración de la interfase entre los ambientes interno y externo.

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:** este paso es muy importante, dado que todos los riesgos que se identifiquen deben tener impacto en el cumplimiento del objetivo estratégico o del proceso.
- **Identificación de los puntos de riesgo:** son actividades dentro del flujo del proceso donde existe evidencia o se tienen indicios de que pueden ocurrir eventos de riesgo operativo y deben mantenerse bajo control para asegurar que el proceso cumpla con su objetivo.
- **Identificación de áreas de impacto:** el área de impacto es la consecuencia económica o reputacional a la cual se ve expuesta la entidad en caso de materializarse un riesgo. Los impactos que aplican son afectación económica (o presupuestal) y reputacional.
- **Identificación de áreas de factores de riesgo:** son las fuentes generadoras de riesgos. Algunos factores de riesgo que puede tener la entidad son:

Tabla 5 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 de cálculos para pagos internos y externos.

riesgo. Se debe tener en cuenta que para un mismo riesgo pueden existir más de una causa o subcausas que pueden ser analizadas.

Premisas para una adecuada redacción del riesgo:

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

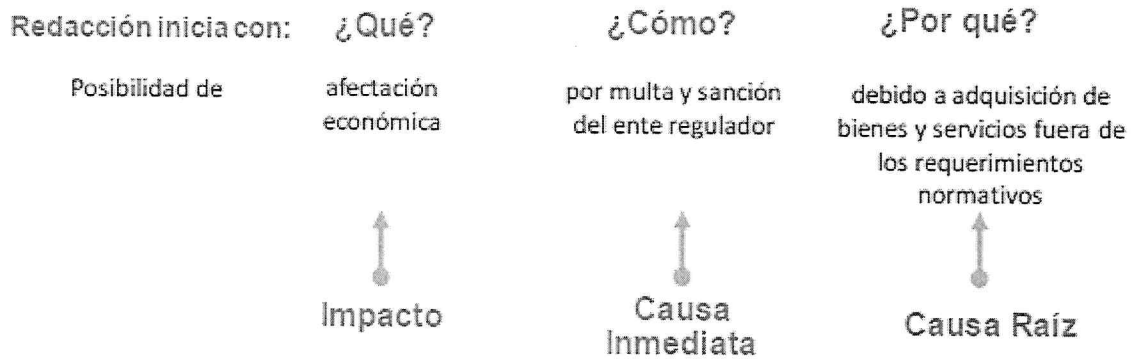
- No describir causas como riesgos.
  Ejemplo: inadecuado funcionamiento de la plataforma estratégica donde se realiza el seguimiento a la planeación.

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

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

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

Ilustración 5 Ejemplo Aplicado Bajo la Estructura Propuesta para la Redacción del Riesgo



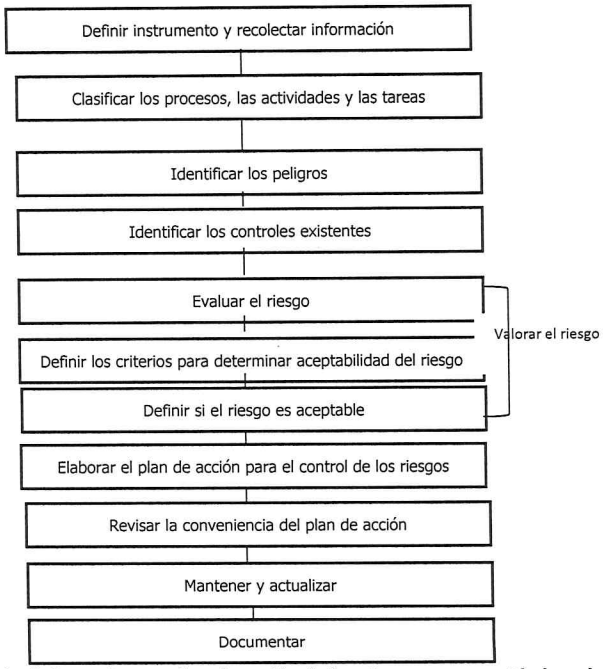
Fuente: Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas - versión 5

Clasificación del Riesgo

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

- 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, cuando y como 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 son 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 7 Identificación de los Peligros y la Valoración de los Riesgos



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

- ¿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.

7.2.2. 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, ya que 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 9 Ejemplo Tipos de Fuentes de Impactos

Fuente		Ruta	Barrera	Receptor	Impacto
Peligro/aspecto	Evento				
Fuente de energía:	Falla de planta.	Dispersión y deposición atmosférica.	Física	Humano	Medidas relacionadas con:
-Química	Liberación tóxica.	Superficie	De Procesamiento Administrativa Reglamentaria	Social	-Sostenibilidad
-Eléctrica	Fuego	acuática:		Económico	-Seres Humanos
-Mecánica	Contaminación	-Drenaje local y escurrimiento,		Instalaciones	-Sociedad
-Por presión	Limpieza de la tierra	-Corrientes y sistemas, hidrológicos,		Patrimonio	-Economía

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.

7.2.3. 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

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.
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.
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).

Tabla 10 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: Guía para la identificación y declaración del conflicto de intereses en el sector público colombiano- versión 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
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

Fuente: Guía para la identificación y declaración del conflicto de intereses en el sector público colombiano

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 13 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

Proceso, Procedimiento o Actividad	Factores de Riesgos
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 5

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

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

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

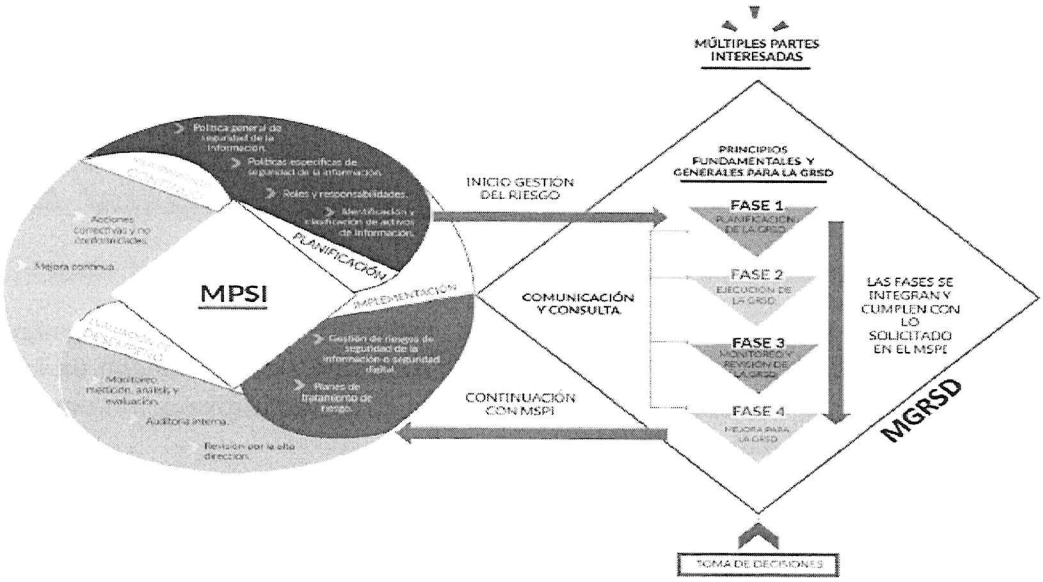
Las preguntas clave para la identificación del riesgo son:

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

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

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

Ilustración 7 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 d, 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.

7.2.6.1. Identificación de activos de Seguridad Digital

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

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

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

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 16 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) o Ambientales(A)

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

Tipo	Vulnerabilidades
	Ausencia de políticas de uso aceptable
	Trabajo no supervisado de personal externo o de limpieza
Lugar	Uso inadecuado de los controles de acceso al edificio
	Áreas susceptibles a inundación
	Red eléctrica inestable
	Ausencia de protección en puertas o ventanas
Organización	Ausencia de procedimiento de registro/retiro de usuarios
	Ausencia de proceso para supervisión de derechos de acceso
	Ausencia de control de los activos que se encuentran fuera de las instalaciones
	Ausencia de acuerdos de nivel de servicio (ANS o SLA)
	Ausencia de mecanismos de monitoreo para brechas en la 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 pueda 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, ya que se puede determinar con claridad la frecuencia con la que se lleva a cabo una actividad, en vez de considerar los posibles eventos que pudiesen haberse dado en el pasado, ya que, bajo esta óptica, si nunca se han presentado eventos, todos los riesgos tendrán la tendencia a quedar ubicados en niveles bajos, situación que no es real frente a la gestión de las entidades públicas colombianas.

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

Tabla 20 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
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 21 Criterios para Definir el Nivel de Impacto

	Afectación Económica	Reputacional
Leve 20%	Afectación menor a 10 SMLMV	El riesgo afecta la imagen de algún área de la 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 5

- **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

Tabla 23 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.

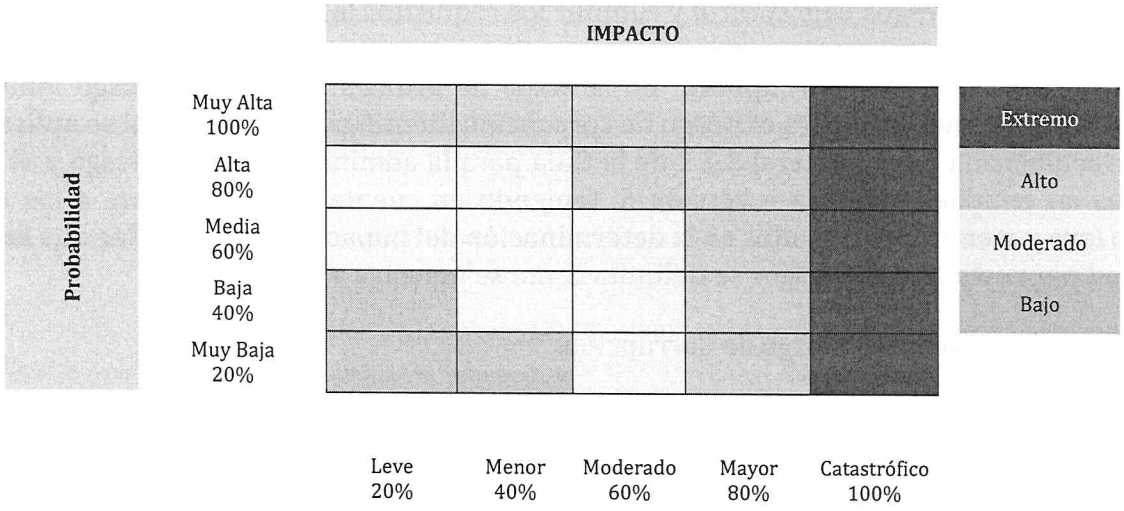
Niveles	Descripción Impacto (Consecuencias) Cuantitativo	Descripción Impacto (Consecuencias) Cualitativo
	- Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la Entidad en un valor ≥50%. - Pago de sanciones económicas por incumplimiento en la normatividad 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: para la determinación del impacto frente a posibles materializaciones de riesgos de corrupción, se analizarán únicamente los siguientes niveles i) moderado, ii) mayor, y iii) catastrófico, dado que estos riesgos siempre serán significativos, en tal sentido, no aplican los niveles de impacto leve y menor, que sí aplican para las demás tipologías de riesgos.

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 25 Matriz Valoración Riesgo de Gestión



Fuente: Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas - versión 5

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 deberían 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:

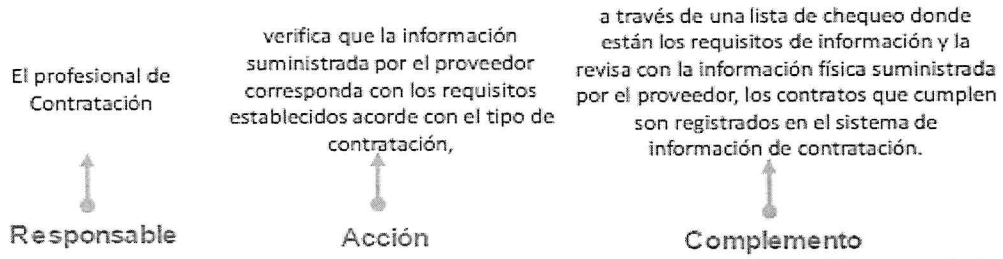
- Situaciones en que los peligros puedan afectar la seguridad o la salud y no haya certeza de que los controles existentes o planificados sean adecuados, en principio o en la práctica;
- Organizaciones que buscan la mejora continua del seguridad y salud en el trabajo y el cumplimiento de los requisitos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

- 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 9 Ejemplo: Estructura para la Redacción del Control



Fuente: Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas - versión 5

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:

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 5

encuentran en el "FORMATO PARA LA DEFINICIÓN, VALORACIÓN, ANÁLISIS Y EVALUACIÓN DE CONTROLES ".

Tabla 28 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	
¿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.

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

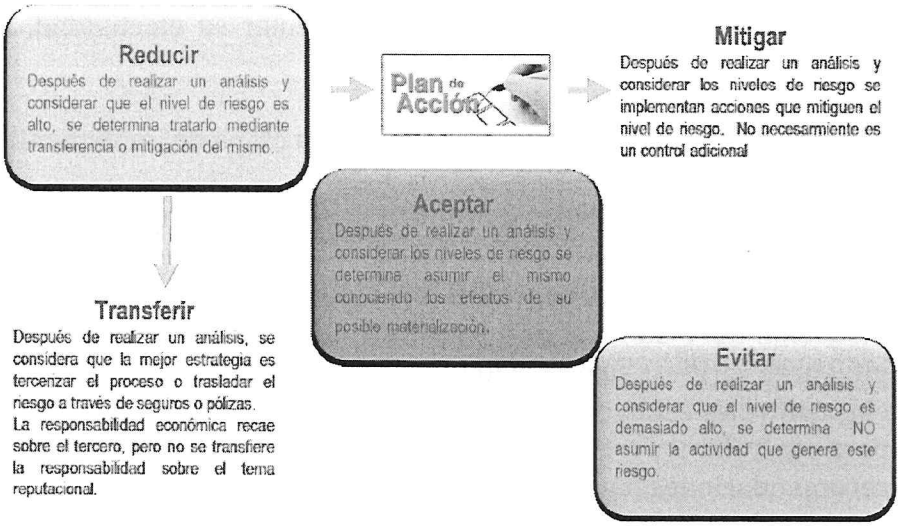
Valoración de controles en riesgos de seguridad digital: la entidad podrá mitigar/tratar los riesgos de seguridad digital empleando como mínimo los controles del Anexo A de la norma técnica ISO/IEC 27001:2013, estos controles se encuentran en el "**Anexo 4 Lineamientos para la Gestión de Riesgos de Seguridad 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 11 Plan de Acción



Fuente: Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas - versión 5

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.

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 la zona de riesgo moderada pueden asumirse (pueden 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.
c. **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.

8. Historia de Cambios del Documento

Versión	Motivo del Cambio	Descripción del Cambio	Fecha del Cambio
1	Versión inicial	Elaboración del documento de política	11 de Enero de 2017
2	Revisión y actualización de la Política de Administración del Riesgo	Revisión de la Política de Administración de Riesgos, respecto a los cambios normativos establecidos en el Decreto 648 de 2017 y en la Guía para la administración del riesgo del y el diseño de controles en entidades públicas. Riesgos de gestión, corrupción y seguridad digital. Versión 4. Octubre de 2018.	19 de Diciembre de 2018
3	Revisión y actualización con base en la nueva guía metodológica emitida por el DAFP.	Se actualiza la Política de Administración del riesgo de acuerdo con los lineamientos establecidos por el Departamento Administrativo de la Función Pública – DAFP, a través de la "Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 5, diciembre de 2020".	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.	25 de Agosto de 2022