Guía de administración del riesgo

Proceso: Administración del Sistema Integrado de Gestión

Versión 9

17/07/2024

TABLA DE CONTENIDO

1 PRESENTACIÓN

El Ministerio de Ambiente y Desarrollo Sostenible como entidad del orden público se encuentra expuesta a una serie de factores de tipo externo e interno que pueden poner en riesgo el cumplimiento de su misión y objetivos institucionales, así como el desarrollo eficiente y efectivo de sus procesos; por ende se hace necesario realizar el análisis del contexto e implementar una guía metodológica que permita identificar, evaluar, valorar y definir el tratamiento encaminado al manejo de los impactos generados.

Es importante así mismo el cumplimiento de requisitos de orden normativo contemplados a través del Decreto 1537 de 2001 en donde se establece la identificación y el análisis de riesgos como un proceso permanente e interactivo entre las oficinas de control interno y la administración, y deja a la vista la responsabilidad que deben adquirir los encargados de los procesos en la aplicación de las políticas de tratamiento definidas. En este sentido, el Decreto 1599 de 2005 adopta el Modelo Estándar de Control Interno – MECI para todas las entidades del Estado, en donde se contempla a la administración del riesgo dentro del Subsistema de Control Estratégico. Valiéndose de elementos como la misión, la visión, los objetivos, los valores y las estrategias para promover el compromiso de la dirección e involucrarse en todos los procesos de la entidad. Este modelo fue actualizado a través de los decretos 943 de 2014 y 1499 de 2017.

Por otra parte, una vez la entidad estructure su sistema de administración de riesgos, éste: contribuye al logro de los objetivos institucionales y al mejoramiento del desempeño organizacional a través de la generación de una cultura del riesgo, define una base confiable para la planeación y la toma de decisiones, involucra a todos los procesos y el talento humano de la entidad y promueve el mejoramiento continuo a partir del seguimiento, la revisión y el establecimiento de metas de desempeño institucional, dirigidas a mejorar la calidad de los servicios ofertados y la eficacia de las operaciones realizadas.

A continuación, se describen las etapas para la identificación, análisis, evaluación y tratamiento de los riesgos vinculados con los procesos del Sistema Integrado de Gestión del Ministerio de Ambiente y Desarrollo Sostenible y aquellos que por disposición de la Ley 1474 de 2011 son denominados riesgos de corrupción.

2 OBJETIVO

Establecer los lineamientos metodológicos para llevar a cabo la identificación, análisis, evaluación y tratamiento de riesgos por procesos con miras a generar el Mapa de Riesgos del Ministerio de Ambiente y Desarrollo Sostenible.

3 ALCANCE

La administración del riesgo aplica para todos los procesos del Sistema Integrado de Gestión (estratégicos, misionales, de apoyo y de evaluación independiente) que operan en la sede del Ministerio de Ambiente y Desarrollo Sostenible. Inicia con la identificación de los riesgos y termina con su monitoreo y seguimiento, con el fin de evidenciar el cumplimiento de las acciones planteadas.

4 DEFINICIONES O CONCEPTOS

- **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.

- **AMENAZA:** Situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización.

- **ANÁLISIS DEL RIESGO**: Proceso para comprender la naturaleza del riesgo y determinar el nivel del riesgo.

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

- **BIEN PÚBLICO**: Son todos aquellos muebles e inmuebles de propiedad pública (este concepto comprende: bienes del Estado y aquellos productos del ejercicio de una función pública a cargo de particulares). Estos se clasifican en bienes de uso público y bienes fiscales, definidos así:
  a) Bien de uso público: aquellos cuyo uso pertenece a todos los habitantes del territorio nacional. Ejemplos: Las calles, plazas, puentes, vías, parques etc.
  b) Bienes fiscales: aquellos que están destinados al cumplimiento de las funciones públicas o servicios públicos (Consejo de Estado, 2012), es decir, afectos al desarrollo de su misión y utilizados para sus actividades. Ejemplos: Los terrenos, edificios, oficinas, colegios, hospitales, otras construcciones, fincas, granjas, equipos, enseres, mobiliario etc.

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

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

- **CAUSA RAÍZ:** Causa principal o básica, corresponde a las razones por la cuales se puede presentar el riesgo.

- **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.

- **CONFIDENCIALIDAD:** Propiedad de la información que la hace no disponible, es decir, divulgada a individuos, entidades o procesos no autorizados.

- **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.

- **CONTEXTO ESTRATÉGICO**: conjunto de circunstancias internas y externas que puedan generar eventos que originen oportunidades o afecten el cumplimiento de su función, misión y objetivos institucionales.

- **CONTROL:** Medida que permite reducir o mitigar un riesgo (procesos, políticas, dispositivos, prácticas u otras acciones).

- **CRITERIOS DE RIESGOS:** Términos de referencia sobre los cuales se evalúa la importancia de un riesgo. Estos criterios se definen con base en los objetivos de la organización y en el contexto interno y externo.

- **DISPONIBILIDAD:** Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada. ISO 27000.

- **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

- **EVALUACIÓN DEL RIESGO**: Proceso de la comparación de los resultados del análisis con los criterios del riesgo, para determinar si el riesgo, su magnitud o ambos son aceptables o tolerables.

- **FACTORES DE RIESGO:** Son las fuentes generadoras de riesgos.

- **GESTIÓN 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.

- **GESTOR FISCAL:** Son los servidores públicos y las personas de derecho privado que manejen o administren recursos o fondos públicos, desarrollando actividades económicas, jurídicas y tecnológicas,

tendientes a la adecuada y correcta adquisición, planeación, conservación, administración, custodia, explotación, enajenación, consumo, adjudicación, gasto, inversión y disposición de los bienes públicos, así como, a la recaudación, manejo e inversión de sus rentas, en orden a cumplir los fines esenciales del Estado (artículo 3 de la Ley 610 de 2000 o la norma que lo sustituya o modifique). A título de ejemplo son gestores fiscales, entre otros (sin perjuicio de las particularidades de cada entidad): representante legal, ordenador del gasto, autorizado para contratar, pagador, tesorero, almacenista.

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

- **IDENTIFICACIÓN DEL RIESGO**: Proceso que posibilita conocer los eventos potenciales, que estén o no bajo el control de la organización, para ello se debe tener en cuenta el contexto estratégico en el que opera la entidad, la caracterización de cada proceso que contempla su objetivo y alcance y, también, el análisis frente a los factores internos y externos que pueden generar riesgos que afecten el cumplimiento de los objetivos.

- **IMPACTO:** Se entiende como las consecuencias que puede ocasionar a la organización la materialización del riesgo.

- **INCIDENTE:** Evento o serie de eventos de seguridad digital no deseados o inesperados, que tienen probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

- **INTEGRIDAD:** Propiedad de la información relativa a su exactitud y completitud. ISO 27000.

- **INTERESES PATRIMONIALES DE NATURALEZA PÚBLICA:** Son expectativas razonables de beneficios, que en condiciones normales se espera obtener o recibir y que sean susceptible de estimación económica. A diferencia del recurso público, los intereses patrimoniales de naturaleza pública son expectativas. Ejemplos: la rentabilidad proyectada de cualquier inversión pública, es decir antes de que se causen o generen efectivamente; la cobertura de garantías y pólizas; la participación accionaria pública en una empresa de economía mixta o en una empresa de servicios públicos con socio o socios públicos; los rendimientos financieros y frutos de recursos públicos cuando se proyectan, es decir antes de que se causen o generen efectivamente; así como, los intereses moratorios, indexaciones, actualización del dinero en el tiempo, estimación de pérdida de costo de oportunidad, cuando se trata de cobrar recursos públicos que un tercero debe; explotación de bienes públicos y/o recaudo de recursos públicos por un particular sin contrato o habilitación legal.

- **MAPA DE RIESGOS:** Documento con la información resultante de la gestión del riesgo.

- **NIVEL DE RIESGO:** Es el valor que se determina a partir de combinar la probabilidad de ocurrencia de un evento potencialmente dañino y la magnitud del impacto que este evento traería sobre la capacidad institucional de alcanzar los objetivos.

- **POLÍTICAS DE ADMINISTRACIÓN DE RIESGOS**: Declaración de la dirección y las intenciones generales de una organización con respecto a la gestión del riesgo (NTC ISO 31000 Numeral 2.4). La gestión o administración del riesgo establece lineamientos precisos acerca del tratamiento, manejo y seguimiento a los riesgos.

- **PROBABILIDAD:** Se entiende la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. La probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año.

- **PROCESO:** Sistema de actividades que utilizan recursos para transformar entradas en salidas.

- **PROPIETARIO DEL RIESGO:** Persona o entidad con responsabilidad y autoridad para gestionar un riesgo.

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

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

- **RIESGO AMBIENTAL:** Posibilidad de que por forma natural o por acción humana se produzca impacto en el medio ambiente.

- **RIESGO DE CORRUPCIÓN:** Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.

- **RIESGO DE GESTIÓN:** Posibilidad de que suceda algún evento que tendrá un impacto sobre el cumplimiento de los objetivos.

- **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 FISCAL:** Efecto dañoso sobre recursos públicos o bienes o intereses patrimoniales de naturaleza pública, a causa de un evento potencial (acción u omisión)

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

- **RIESGO RESIDUAL:** El resultado de aplicar la efectividad de los controles al riesgo inherente.

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

- **VALOR DEL ACTIVO**: Está determinado por el valor de la confidencialidad, integridad y disponibilidad del activo de información.

- **VALORACIÓN DEL RIESGO**: Proceso global de identificación, análisis y evaluación del riesgo.

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

5 MARCO REGULATORIO O NORMATIVO

- Ley 87 de 1993. Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del estado y se dictan otras disposiciones.

- Ley 1474 de 2011. Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.

- Decreto 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.

- Directiva Presidencial 09 de 1999. Lineamientos para la implementación de la política de lucha contra la corrupción.

- NTC ISO 31000 Gestión del riesgo - Directrices

- NTC ISO 27000 Tecnología de la información. técnicas de seguridad. sistemas de gestión de seguridad de la información (SGSI). visión general y vocabulario.

- NTC ISO 27001:2013 Tecnología de la información. técnicas de seguridad. sistemas de gestión de la seguridad de la información. Requisitos

- Plan Anticorrupción Programa de Transparencia y Ética Pública

- Guía para la Administración del Riesgo y el Diseño de Controles en entidades Públicas-DAFP 2022

6 RESPONSABILIDAD

Esta guía establece los lineamientos para la formulación del mapa de riesgos institucional siguiendo los lineamientos del Departamento Administrativo de la Función Pública -DAFP, mediante el diligenciamiento del formato F-E-SIG-28 Mapa de riesgos institucional y su consolidación mediante el documento soporte DS-E-SIG-25 Mapa de riesgos institucional.

Todos los líderes de los procesos definidos en el Sistema Integrado de Gestión del Ministerio, con su equipo de trabajo, serán responsables de la aplicación de esta metodología, la implementación de los controles definidos y su seguimiento, con el apoyo permanente de la Oficina Asesora de Planeación.

La responsabilidad en la implementación de los controles y acciones asociadas a la gestión del riesgo estará definida a partir de roles y no definir nombres específicos de los colaboradores.

Así mismo, la Oficina de Control Interno verificará el cumplimiento e implementación de esta guía en los procesos definidos por la entidad y la medición de la eficacia de las acciones y controles que permitan contrarrestar la materialización de los riesgos identificados. Para la actualización del mapa de riesgos institucional se tendrán en cuenta dichas observaciones y analizar los resultados de las evaluaciones llevadas a cabo por los organismos de control.

Para el establecimiento e implementación de un Sistema de Administración de Riesgos es necesario contar con el compromiso y la definición de responsabilidades desde el Despacho del Ministerio y Viceministerios hacia todos los niveles de la entidad, por lo que se presentarán en el Comité Institucional de Gestión y Desempeño. los resultados de los seguimientos y monitoreos realizados al mapa de riesgos.

Para esto, la alta dirección debe designar al representante de la alta dirección para apoyar a los líderes de procesos y demás servidores quienes son en última instancia los encargados de identificar y elaborar el mapa de riesgos.

Cuando se requiera la actualización de la presente Guía, se liderará el proceso por parte de la Oficina Asesora de Planeación con la asesoría de la Oficina de Control Interno y la participación de dependencias líderes, de acuerdo con los tipos de riesgo definidos. Es decir, los riesgos de gestión y de corrupción serán liderados por la Oficina Asesora de Planeación, los riesgos de seguridad de la información por la Oficina de Tecnologías de la Información y la Comunicación- OTIC, los riesgos ambientales por las dependencias líderes del Sistema de Gestión Ambiental, como lo son, Subdirección Administrativa y Financiera (grupo de servicios administrativos) en conjunto con la Oficina Asesora de Planeación (grupo de Gestión y Desempeño Institucional) y de acuerdo a la necesidad de incluir nuevos riesgos se convocarán a las dependencias involucradas de acuerdo a sus competencias.

7 METODOLOGÍA PARA LA ADMINISTRACIÓN Y GESTIÓN DEL RIESGOS.

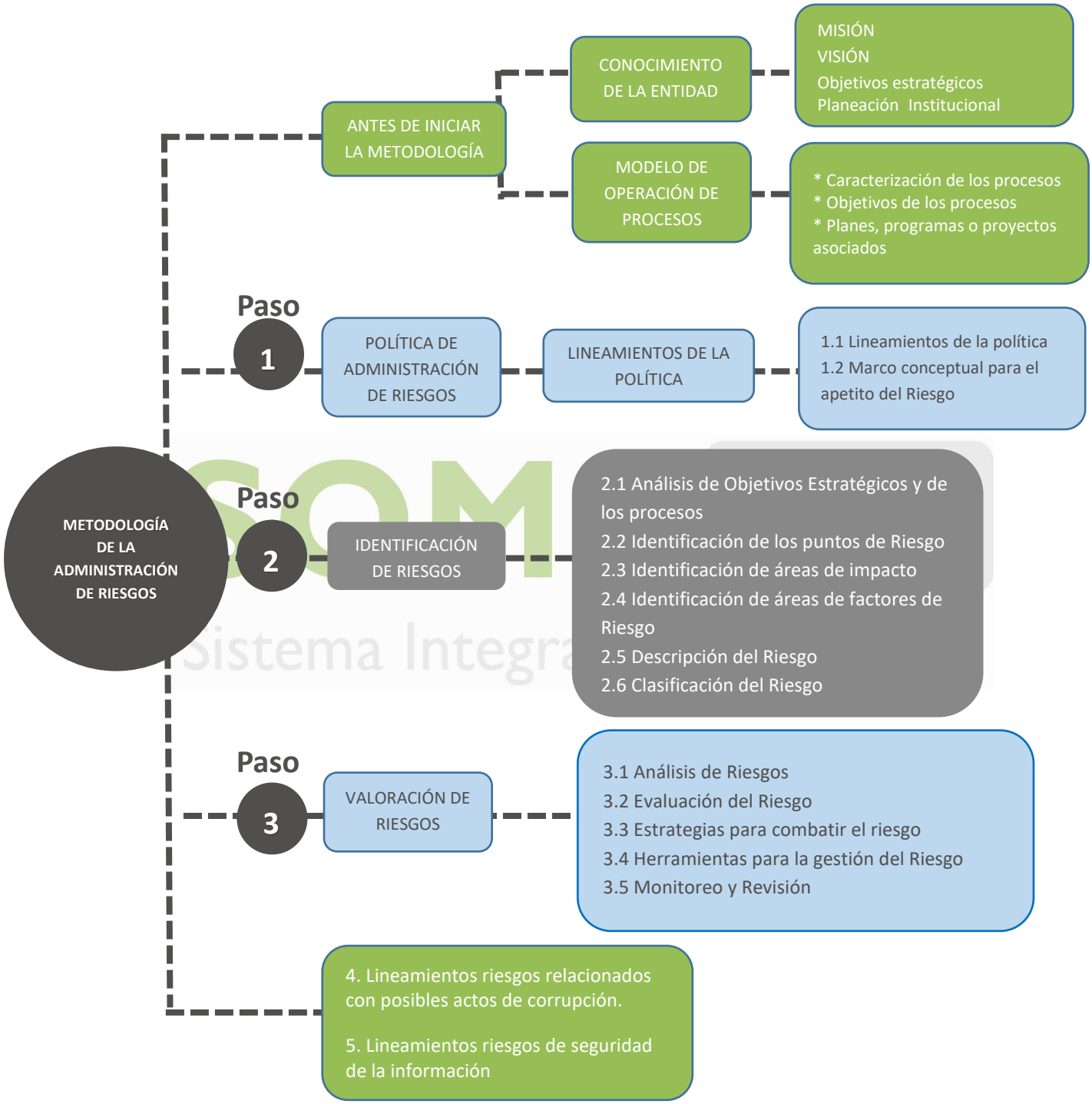


***Diagrama 1**. Metodología para la Administración del Riesgo. Fuente: Guía para la Administración del Riesgo y el Diseño de Controles en entidades Públicas-DAFP. 2020*

7.1 POLÍTICA DE ADMINISTRACIÓN Y GESTIÓN DE RIESGOS

La Alta Dirección del Ministerio de Ambiente y Desarrollo Sostenible en conocimiento de la responsabilidad e importancia del manejo de los riesgos asociados a los diferentes procesos del Sistema Integrado de Gestión, implementa esta Guía por medio de la cual se valoran y se hace tratamiento a los riesgos por procesos como herramienta estratégica y de gestión que permita anticipar y responder de manera oportuna y óptima a la materialización de los riesgos identificados en la matriz, contribuyendo al cumplimiento de los objetivos misionales y la mejora continua del sistema.

Así mismo, la Política de Administración y Gestión de Riesgos será publicada y comunicada a todos los funcionarios y colaboradores del Ministerio de Ambiente y Desarrollo Sostenible a través de los diferentes medios con que cuenta la entidad.

7.1.1 OBJETIVOS DE LA POLÍTICA

- Controlar a través del Mapa de Riesgos todo el proceso relacionado con el manejo de los riesgos asociados al Sistema Integrado de Gestión.
- Proporcionar al Ministerio las directrices para la administración de los riesgos asociados a los procesos de la entidad, con el propósito de contribuir a la adecuada identificación, análisis, valoración (riesgos y controles) y tratamiento de los mismos.
- Integrar el manejo de los riesgos de gestión, corrupción, ambientales y seguridad de la información.
- Establecer la responsabilidad de los diferentes líderes de los procesos del ministerio.
- Establecer el rol de las diferentes dependencias del Ministerio.
- Dar cumplimiento a los requerimientos legales que apliquen al manejo de riesgos de gestión, corrupción, ambientales y de seguridad de la información.
- Fortalecer el comportamiento profesional y personal de los funcionarios del Ministerio de Ambiente y Desarrollo Sostenible.

7.1.2 DETERMINACIÓN DE LA CAPACIDAD DE RIESGO

El Ministerio de Ambiente y Desarrollo Sostenible con la participación y aprobación de la alta dirección en el marco del Comité Institucional de Coordinación de Control Interno debe realizar el análisis de eventos y riesgos críticos que tienen un nivel de severidad muy alto frente a los cuales se deben tomar decisiones, teniendo en cuenta los siguientes valores:

- Valor máximo de la escala que resulta de combinar la probabilidad y el impacto.
- Valor máximo del nivel de riesgo que la entidad puede soportar y a partir del cual se considera por la alta dirección que no sería posible el logro de los objetivos de la entidad que corresponde a la “capacidad de riesgo”.

7.1.3 DETERMINACIÓN DEL APETITO DE RIESGO

Se debe así mismo, determinar el "apetito de riesgo", equivalente al nivel de riesgo que la entidad puede aceptar, relacionado con sus objetivos, el marco legal y las disposiciones de la alta dirección en condiciones normales de operación del Modelo Integrado de Planeación y Gestión en la entidad.

El apetito de riesgo puede ser diferente para los distintos tipos de riesgos de la entidad, se debe tener en cuenta que los riesgos de corrupción son inaceptables.

7.1.4 TOLERANCIA DE RIESGO

El límite o valor de la tolerancia de riesgo es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del apetito de riesgo determinado. Se debe definir un valor que es igual o superior al apetito de riesgo y menor o igual a la capacidad, el cual es definido por la alta dirección y aprobada por el órgano de gobierno respectivo.

La determinación de la tolerancia de riesgo es optativa para la entidad y su uso está limitado a determinar el tipo de acciones para abordar los riesgos, dado que las acciones que se desprendan a partir del análisis de riesgos deben ser proporcionadas y razonables, lo cual se puede determinar en función del valor del nivel de riesgo residual obtenido y su comparación con el apetito y tolerancia de riesgo.

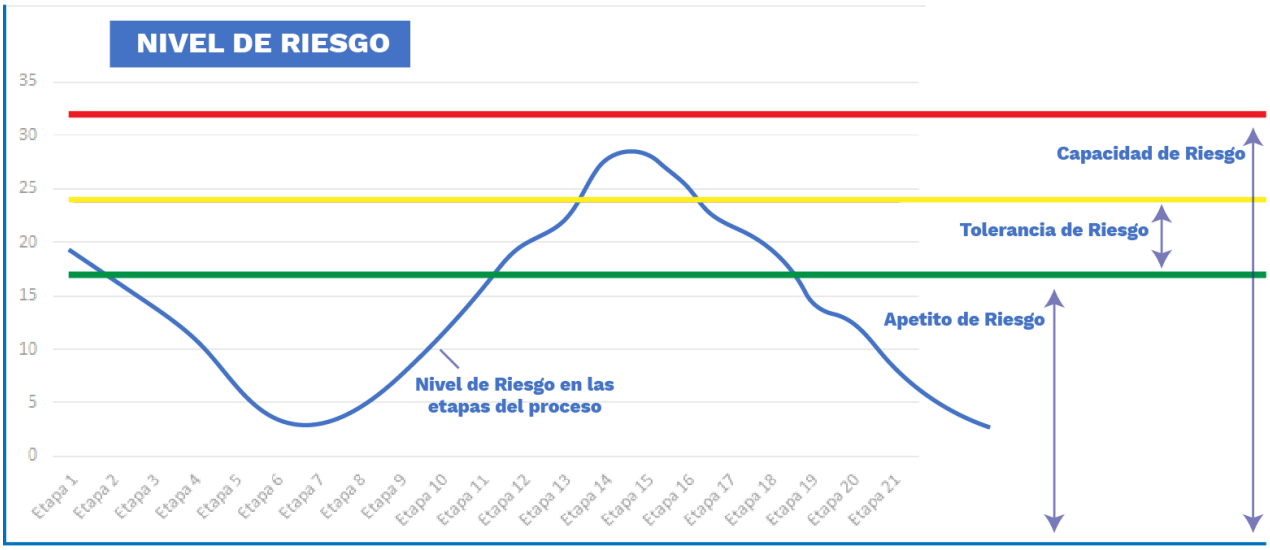


***Diagrama 2**. Apetito, tolerancia y capacidad de riesgo. Fuente: Guía para la Administración del Riesgo y el Diseño de Controles en entidades Públicas-DAFP. 2020. Tomado de la guía de buenas prácticas de gestión de riesgos del Instituto de Auditores Internos (IIA GLOBAL), junio de 2013*

7.2 IDENTIFICACIÓN DEL RIESGO

En esta etapa se deben establecer las fuentes o factores de riesgo, los eventos o riesgos, sus causas y sus consecuencias. Para el análisis se pueden involucrar datos históricos, análisis teóricos, opiniones informadas y expertas y las necesidades de las partes involucradas.

7.2.1 ANÁLISIS DE OBJETIVOS ESTRATÉGICOS Y DE LOS PROCESOS

Los riesgos identificados deben tener impacto en el cumplimiento de objetivos estratégicos, estar alineados con la misión y la visión institucional, así como, su desdoble hacia los objetivos de los procesos.

Para su adecuada formulación, deben contener unos atributos mínimos, para lo cual se puede hacer uso de las características SMART:

S	Specific - Específico	Resuelve cuestiones como qué, cuándo, cómo, dónde, con qué, quién considerando el orden y los necesarios para el cumplimiento de la misión.
M	Mesurable - Medible	Involucra algunos números en su definición. Ejemplo: porcentajes o cantidades cuando aplique
A	Achievable - Alcanzable	Realizar un análisis de los que se ha hecho y logrado hasta el momento para determinar si lo que se propone es posible o cómo resultaría mejor
R	Relevant - Relevante	Considera recursos, factores externos e información de actividades previas
T	Timely -Temporal	Establecer un tiempo al objetivo ayudará a saber si lo que se está haciendo es lo óptimo para llegar a la meta, así mismo permite determinar el cumplimiento y las mediciones finales.

Tabla 1. *Características SMART. Adaptada fuente: DAFP. 2018.*

De acuerdo con lo anterior, se debe tener en cuenta que los indicadores del Sistema Integrado de Gestión- SIG, permiten medir el cumplimiento del objetivo de cada proceso, alineados con la plataforma estratégica del SIG (Objetivos, política, misión y visión) y de la misma manera los riesgos se identifican a partir de los factores de riesgo que puedan afectar el cumplimiento del objetivo de cada proceso.

7.2.2 IDENTIFICACIÓN DE LOS PUNTOS DE RIESGO

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.

Para identificar estos puntos de riesgo es importante tener en cuenta la documentación del proceso: caracterización, contexto estratégico, procedimientos, guías, protocolos, manuales, instructivos, documentos soporte y formatos, entre otros. Así como, la cadena de valor público, desde insumos, procesos, productos, resultados, efectos e impactos y el cumplimiento de los objetivos (eficacia y eficiencia).

Para la identificación del riesgo fiscal, los puntos de riesgo, pueden incluir actividades de gestión fiscal (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), así mismo, se deben tener en cuenta aquellas actividades en las cuales se han generado advertencias, alertas, hallazgos fiscales o fallos con responsabilidad fiscal.

7.2.3 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.

Dentro del contexto de riesgo fiscal, el área de impacto siempre corresponderá a una consecuencia económica sobre el patrimonio público sobre: recursos públicos, bienes públicos o intereses patrimoniales de naturaleza pública.

7.2.4 IDENTIFICACIÓN DE ÁREAS DE FACTORES DE RIESGO

Son las fuentes generadoras de riesgos, las cuales se documentan en los contextos estratégicos por proceso.

Corresponde a la definición de los parámetros internos y externos que se han de tomar en consideración para la administración del riesgo.

De igual manera, todas las actividades internas y del entorno, que pueden generar eventos que originan oportunidades o afecten negativamente el cumplimiento de la misión y objetivos.

CONTEXTO EXTERNO: Se determinan las características o aspectos esenciales del entorno en el cual opera la entidad	**ECONÓMICOS:** Disponibilidad de capital, liquidez, mercados financieros, desempleo, competencia
	MEDIOAMBIENTALES: Emisiones y residuos, energía, catástrofes naturales, desarrollo sostenible
	POLÍTICOS: Cambios de gobierno, legislación, políticas públicas, regulación, normatividad externa (leyes, decretos, ordenanzas y acuerdos).
	SOCIALES: Demografía, responsabilidad social, orden público.
	TECNOLÓGICOS: Avances en tecnología, acceso a sistemas de información externos, gobierno en línea, Innovación.
	COMUNICACIÓN EXTERNA: Mecanismos utilizados para entrar en contacto con los usuarios o ciudadanos, canales establecidos para que el mismo se comunique con la entidad

CONTEXTO INTERNO: Se determinan las características o aspectos esenciales del ambiente en cual la organización busca alcanzar sus objetivos.	**FINANCIEROS:** Presupuesto de funcionamiento, recursos de inversión, infraestructura, capacidad instalada
	PERSONAL: Competencia del personal, disponibilidad del personal, seguridad y salud ocupacional
	PROCESOS: Capacidad, diseño, ejecución, proveedores, entradas, salidas, gestión del conocimiento.
	TECNOLOGÍA: Integridad de datos, disponibilidad de datos y sistemas, desarrollo, producción, mantenimiento de sistemas de información, información, aplicaciones, hardware entre otros, que se deben proteger para garantizar el funcionamiento interno de cada proceso, como de cara al ciudadano.
	ESTRATÉGICOS: Direccionamiento estratégico, planeación institucional, liderazgo, trabajo en equipo
	COMUNICACIÓN INTERNA: Canales utilizados y su efectividad, flujo de la información necesaria para el desarrollo de las operaciones.
CONTEXTO DEL PROCESO: Se determinan las características o aspectos esenciales del proceso y sus interrelaciones.	**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.
	RESPONSABILIDAD DEL PROCESO: Grado de autoridad y responsabilidad de los funcionarios frente al proceso.
	COMUNICACIÒN ENTRE LOS PROCESOS: Efectividad en los flujos de información determinados en la interacción de los procesos.

Tabla 2. *Factores para cada categoría del contexto. Adaptada fuente: DAFP. 2018*

7.2.5 DESCRIPCIÓN DE RIESGOS

La identificación del riesgo de gestión se realiza determinando las causas, con base en el contexto interno, externo y del proceso ya analizado para el ministerio, y que pueden afectar el logro de los objetivos.

Algunas causas externas no controlables por la entidad se podrán evidenciar en el contexto correspondiente, para ser tenidas en cuenta en el análisis y valoración del riesgo.

A partir de este levantamiento de causas se procederá a identificar el riesgo, el cual estará asociado a aquellos eventos o situaciones que pueden entorpecer el normal desarrollo de los objetivos del proceso.

Para la descripción del riesgo se propone una estructura que facilita su redacción y claridad que inicia con la frase POSIBILIDAD DE y se analizan los siguientes aspectos:

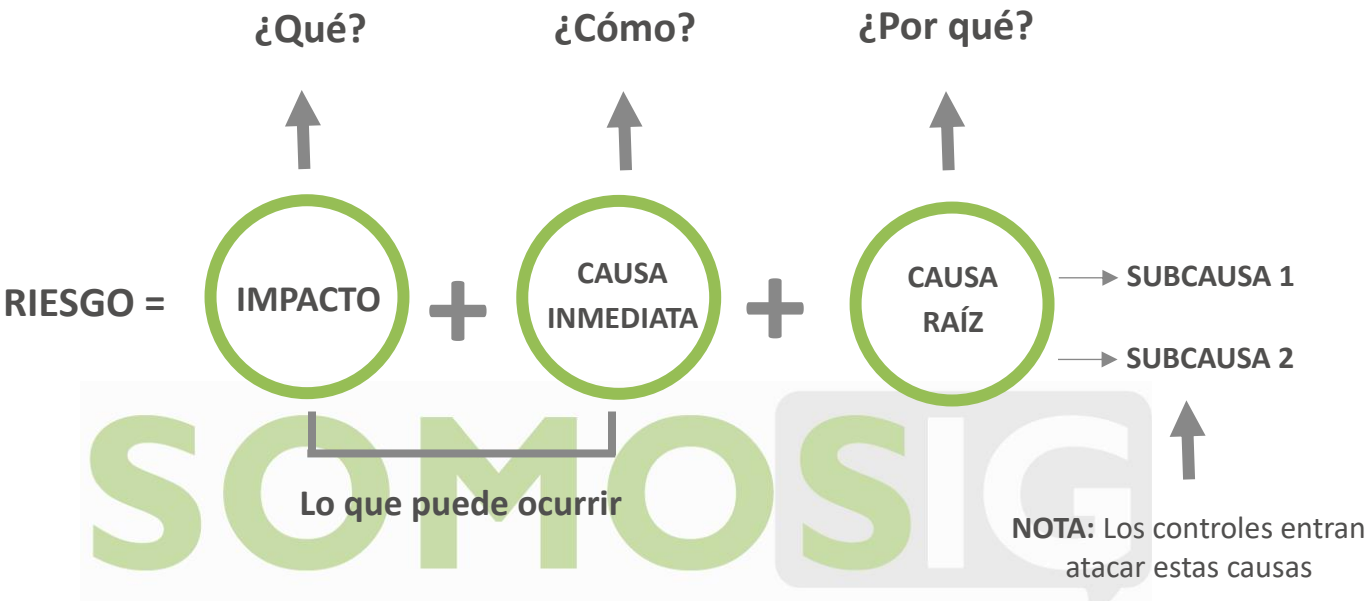


***Diagrama 3**. Estructura propuesta para la redacción del riesgo. Fuente: Guía para la Administración del Riesgo y el Diseño de Controles en entidades Públicas-DAFP. 2020.*

Nota: Para los riesgos de seguridad de la información el campo descripción del riesgo (columna M) del instrumento F-E-SIG-28 - Mapa de riesgos institucional, se encuentra automatizado de acuerdo con la estructura indicada en el diagrama 3

***Diagrama 4**. 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-DAFP. 2020.*

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

Redacción Inicia con:	¿Qué?	¿Cómo?	¿Por qué?
Posibilidad de	efecto 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
	efecto dañoso sobre **recursos públicos**	por sobrecostos en contratos de la entidad	a causa de la omisión del deber de elaborar estudios de mercado
	efecto dañoso sobre **intereses patrimoniales de naturaleza pública**	por no tener incluidos todos los bienes muebles e inmuebles de la entidad en el contrato de seguro	a causa de la omisión en la actualización de bienes que cubren de dicho contrato.
	IMPACTO	CAUSA INMEDIATA	CAUSA RAÍZ

Diagrama 5. *Ejemplo aplicado bajo la estructura propuesta para la redacción del riesgo fiscal. Fuente: Guía para la Administración del Riesgo y el Diseño de Controles en entidades Públicas-DAFP. 2022.*

Donde:

- Impacto: las consecuencias que puede ocasionar a la organización la materialización del riesgo (Económico, Reputacional, Económico y Reputacional)

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

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

Con el fin de facilitar la identificación de **riesgos de corrupción** y evitar que se confunda con un riesgo de gestión, se debe verificar si cumple con los siguientes criterios.

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

Tabla 3. *Matriz para la definición de riesgos de corrupción. Fuente: Secretaría de Transparencia de la Presidencia de la República.*

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

Como primer paso para la identificación de riesgos de seguridad de la información es necesario identificar los activos de información de los procesos del Ministerio para el Sistema de Gestión de Seguridad de la Información y de acuerdo con lo establecido en el instructivo I-E-GET-02 "Metodología para la identificación, gestión y clasificación de activos de información", lo que permite determinar qué es lo más importante que la entidad y sus procesos poseen (bases de datos, archivos, servidores web o aplicaciones clave para la prestación del servicio, entre otros) y saber qué es lo que se debe proteger para garantizar su funcionamiento interno y externo, aumentando así su confianza en el uso del entorno digital.

Así mismo, es importante verificar posibles hechos que afecten la disponibilidad, integridad o confidencialidad de la información, a nivel físico o lógico, hardware, software y a nivel de instalaciones locativas o legales que lleven a afectar la información de la entidad o la privacidad de la información de una parte interesada.

Existen tres (3) tipos de riesgos asociados a los activos de información identificados en la Entidad:
- Pérdida de confidencialidad.
- Pérdida de la integridad.
- Pérdida de la disponibilidad.

Para los activos tipo bases de datos se han determinado los siguientes cuatro (4) tipos de riesgos adicionales:

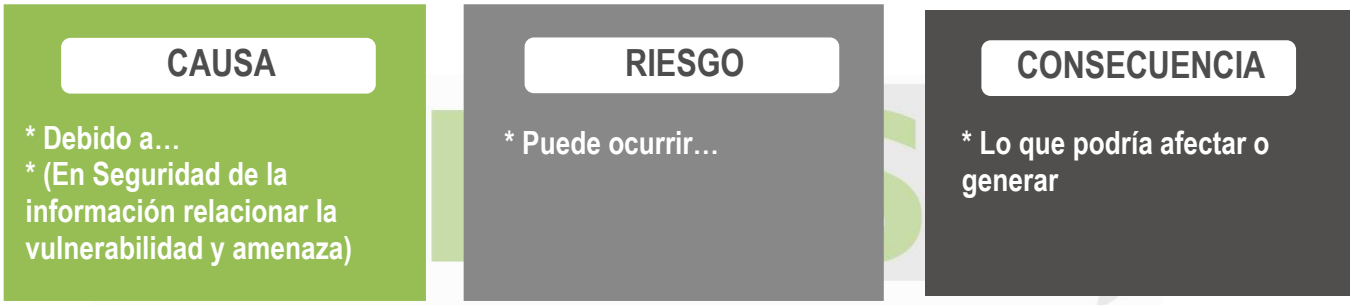
- Posibilidad de pérdida de confidencialidad, divulgación no autorizada o uso inadecuado de la información de datos personales.
- Posibilidad de pérdida de integridad, alteración, o modificación de la información de datos personales.
- Posibilidad de afectación de la disponibilidad de la plataforma tecnológica o aplicativos que gestionan datos personales.
- Posibilidad de sanciones por incumplimiento de las directrices normativas frente a los datos personales.

Es también importante identificar las causas que originan el riesgo con base a la identificación de vulnerabilidades y amenazas. La identificación de las vulnerabilidades de los activos de información son debilidades que son aprovechadas por amenazas y generan un riesgo. Una vulnerabilidad que no tiene una

amenaza, puede no requerir de la implementación de un control, para lo cual es necesario identificar y monitorear los mismos. Es importante tener en cuenta que un control mal diseñado e implementado puede constituir una vulnerabilidad. Las amenazas y vulnerabilidades comunes se deben consultar en el anexo "Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas (Anexo 4 – DAFP)".

Las amenazas son de origen natural o humano y pueden ser accidentales o deliberadas, algunas amenazas pueden afectar a más de un activo generando diferentes impactos. Algunas de las amenazas consideradas en la norma ISO 27005:2008 son: Virus informático y software malicioso, avería de origen físico, errores de monitorización (log's), errores de usuarios, corte de suministro eléctrico, fallas eléctricas, daños por agua, fallo de comunicaciones, degradación de los soportes principales de almacenamiento de información, fenómeno natural, derrame de líquidos o sólidos, fuego, entre otras.

Para llevar a cabo este proceso se recomienda dar respuesta a los siguientes interrogantes:



Premisas para una adecuada redacción del riesgo:

- En la definición del riesgo se debe evitar iniciar con palabras negativas como: "No…", "Que no…", o con palabras que denoten un factor de riesgo (causa) tales como: "ausencia de", "falta de", "poco(a)", "escaso(a)", "insuficiente", "deficiente", "debilidades en…"
- 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.

7.2.6 CLASIFICACIÓN DEL RIESGO

Para la identificación de los riesgos y con el objeto de incorporar toda clase de riesgo asociado con el proceso, con la seguridad digital y con el ambiente, se puede tener en cuenta la siguiente clasificación dada por el

Departamento Administrativo de la Función Pública que permite agrupar los riesgos identificados, en las siguientes categorías.

Tipo	Descripción
Ejecución y administración de procesos	Pérdidas derivadas de errores en la ejecución y administración de procesos. Evaluar información proveniente de la gestión y mesa de asistencia -GEMA frente a los incidentes y casos registrados módulo administrativo (si aplica).
Fraude externo	Pérdida derivada de actos de fraude por personas ajenas a la organización (no participa personal de la entidad).
Fraude interno	Pérdida debido a actos de fraude, actuaciones irregulares, comisión de hechos delictivos abuso de confianza, apropiación indebida, incumplimiento de regulaciones legales o internas de la entidad en las cuales está involucrado por lo menos 1 participante interno de la organización, son realizadas de forma intencional o con ánimo de lucro para sí mismo o para terceros. Evaluar información proveniente de quejas y denuncias de los usuarios y la necesidad de evaluar información proveniente de quejas y denuncias de los servidores de la entidad para la identificación de riesgos de fraude y corrupción
Fallas tecnológicas	Errores en *hardware*, *software*, telecomunicaciones, interrupción de servicios básicos. Evaluar información proveniente de la gestión y mesa de asistencia -GEMA frente a los incidentes y casos registrados módulo de apoyo a nivel tecnológico y de comunicaciones
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.
Fiscal	Efecto dañoso sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública, a causa de un evento potencial
Ambiental	Impacto sobre el medio ambiente, por forma natural o por acción humana. Evaluar información proveniente de la gestión y mesa de asistencia -GEMA frente a los incidentes y casos registrados módulo administrativo (si aplica).
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. Evaluar información proveniente de la gestión y mesa de asistencia -GEMA frente a los incidentes y casos registrados módulo administrativo (si aplica).

Tabla 4. *Clasificación de riesgos Adaptada Fuente: DAFP. 2022.*

7.2.6.1. Riesgos de corrupción

Para su identificación se deben tener en cuenta algunas actividades susceptibles de riesgos de corrupción identificadas en la Guía para la Administración del Riesgo y Diseño de Controles en Entidades Públicas del DAFP, principalmente:

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 áreas de planeación y presupuesto)

- Inclusión de gastos no autorizados.
- Inversiones de dineros públicos en entidades de dudosa solidez financiera, a cambio de beneficios indebidos para servidores públicos encargados de su administración.
- Inexistencia de registros auxiliares que permitan identificar y controlar los rubros de inversión.
- Inexistencia de archivos contables.
- Afectar rubros que no corresponden con el objeto del gasto en beneficio propio o a cambio de una retribución económica.

De 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).
- Disposiciones establecidas en los pliegos de condiciones que dirigen 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.
- Otorgar labores de supervisión a personal sin conocimiento para ello.
- Concentrar las labores de supervisión en poco personal.
- Contratar con compañías de papel que no cuentan con experiencia.

De información y documentación

- Ausencia o debilidad de medidas o políticas de conflictos de interés.
- Concentración de información de determinadas actividades o procesos en una persona.
- Ausencia de sistemas de información.
- Ocultar la información considerada pública para los usuarios.
- Ausencia o debilidad de canales de comunicación
- Incumplimiento de la Ley 1712 de 2014.

De investigación y sanción

- Ausencia o debilidad de canales de comunicación.
- Dilatar el proceso para lograr el vencimiento de términos o la prescripción del mismo.
- Desconocimiento de la ley, mediante interpretaciones subjetivas de las normas vigentes para evitar o postergar su aplicación.
- Exceder las facultades legales en los fallos.

De trámites o servicios internos y externos

- Cobros asociados al trámite.
- Influencia de tramitadores
- Tráfico de influencias: (amiguismo, persona influyente).
- Demorar su realización.

De reconocimiento de un derecho (expedición de licencias o permisos)

- Falta de procedimientos claros para el trámite.
- Imposibilitar el otorgamiento de una licencia o permiso.
- Ofrecer beneficios económicos para aligerar la expedición o para amañar la misma.
- Tráfico de influencias: (amiguismo, persona influyente).

7.2.6.2. Riesgos de seguridad de la información

La identificación y valoración de los **riesgos de seguridad y privacidad de la información** para prevenir o reducir efectos indeseados, lograr la mejora continua, identificar sus consecuencias potenciales y la probabilidad de ocurrencia, así como, la aplicación de los controles establecidos en el anexo A de la ISO 27001, se basan en la afectación de tres criterios en un activo o un grupo de activos dentro del proceso: "Integridad, confidencialidad o disponibilidad".

El enfoque hacia la gestión de riesgos de seguridad de la información, relacionados a los activos de información a partir de la identificación de las vulnerabilidades y amenazas presentes en los mismos y su respectivo análisis de consecuencias, permitirá a su vez la aplicación y seguimiento de los controles previstos, a fin de mitigar los posibles impactos que puede generar la materialización de estos.

Identificación de los activos o grupo de activos de información

Se debe garantizar la identificación de lineamientos relacionados a la detección y prevención del uso inadecuado de información privilegiada u otras situaciones que puedan implicar riesgos para la entidad de acuerdo con lo definido en el formato F-E-GET-18 "Matriz inventario de activos de información Ministerio de Ambiente y Desarrollo Sostenible – AMBIENTE", donde se identifica el nivel de confidencialidad, integridad y disponibilidad requeridos para el manejo de la información de los procesos.

A partir del inventario de activos de información actualizado de cada proceso en el formato F-E-GET-18 "Matriz inventario de activos de información Ministerio de Ambiente y Desarrollo Sostenible – AMBIENTE", se realiza

el análisis de identificación de los riesgos de seguridad y privacidad de la información de acuerdo con la valoración de las amenazas, vulnerabilidades y su respectivo impacto sobre los activos de información.

La evaluación de los riesgos de seguridad y privacidad de la información inicia con la identificación y selección del proceso a intervenir en el formato F-E-SIG-28 Mapa de riesgos institucional, pestaña riesgos de seguridad de la información, para la columna B "Proceso", asociado a la respectiva dependencia, oficina o grupo interno de trabajo **columna C y D**. Es importante contar con la información principal del proceso como su objetivo, alcance, inventario de activos de información y demás documentación del proceso necesarios para la respectiva gestión, evaluación y tratamiento de los riesgos asociados.

En la **columna E,** titulada "NOMBRE DEL ACTIVO / GRUPO DE ACTIVOS", se deberá definir el nombre del activo o grupo de activos.

En la **columna F**, titulada "DESCRIPCIÓN DEL ACTIVO / GRUPO DE ACTIVOS", se debe ingresar el nombre de los activos de información que han sido identificados en el formato F-E-GET-18, "Matriz inventario de activos de información del Ministerio de Ambiente y Desarrollo Sostenible – AMBIENTE". El procedimiento a seguir es el siguiente:

- Filtrar la matriz F-E-GET-18 por el tipo de activo.
- Registrar y consolidar en la misma celda el o los nombres de los activos que se identifiquen como resultado del paso anterior.

En la **Columna G** titulada "Tipo de activo/ grupo de activos" corresponde a los tipos de activos identificados en el F-E-GET-18, los cuales se encuentran clasificados así:

Tipo de Activo	Definición	Ejemplos
Información	Corresponden a este tipo de activos de información, los datos e información almacenada o procesada física o electrónicamente que tiene significado o relevancia para la entidad, en cualquier formato que se genera, almacena, gestiona, transmite.	- **Personales**: Bases y archivo de datos, hojas de vida - **Financieros**: Balances financieros, etc. - **Legales**: Acuerdos de confidencialidad, etc. - **Investigación y desarrollo**: Licencias, estudios, etc. - **Estratégicos**: Planes, indicadores, seguimientos, etc. - **Otros:** Documentación de sistemas de información, copias de seguridad, etc.
Software	Activo informático lógico como programas, herramientas ofimáticas y demás utilizadas para la ejecución de las actividades de la Entidad.	- Sistemas operativos - Herramientas Ofimáticas - Motor de bases de datos - Antivirus - Software Estadístico - Software de Georreferenciación - Motores de bases de datos - Software de diseño y programación - Compiladores

Tipo de Activo	Definición	Ejemplos
Hardware	Corresponden al tipo de activo utilizados para realizar la captura, procesamiento, almacenamiento difusión y divulgación de la información. Se refiere a todos los elementos físicos que permiten el funcionamiento de un medio informático.	- Discos duros o extraíbles - Servidores físicos o virtuales - Computadores - Dispositivos móviles
Servicios	Se relaciona con los servicios tecnológicos proporcionados por la entidad para el apoyo de las actividades de los procesos, las cuales facilitan la administración o el flujo de información.	- Internet - Correo electrónico - Comunicaciones - Directorios compartidos - Aplicaciones - Servicio de correspondencia
Infraestructura física	Recursos requeridos por la entidad para la operación eficaz de los procesos. Corresponden a lugares donde se almacenan o resguardan los sistemas de información y comunicaciones, archivo documental. Espacio o área asignada para alojar y salvaguardar los datos o información considerados como activos críticos para la entidad.	- Edificaciones - Centros de computo - Archivo Central
Recurso Humano	Se refiere a aquellas personas (funcionarios y contratistas) que, por su conocimiento, experiencia, información histórica y criticidad para el proceso, son consideradas activos de información.	- Administradores de infraestructura - Expertos técnicos - funcionarios con memoria institucional - Administradores de seguridad - Proveedores - Consultores
Bases de datos personales	Conjunto de datos y registros que caracterizan a personas naturales o jurídicas	- Base de datos de historias laborales - Base de datos de identificación personal - Base de datos de procedimientos administrativos - Base de datos de salud - Bases de datos de contactos con otras entidades - Bases de datos a inscripción de cursos ofertados por el Ministerio
Infraestructura crítica cibernética	Es la infraestructura soportada por las tecnologías de la Información y por las tecnologías de operación, cuyo funcionamiento es indispensable para la prestación de servicios esenciales para los ciudadanos y para el estado.	- Página Web -Aplicativos de trámites y servicios - Otros

Tabla 5. *Clasificación de activos de información*

7.3 ANÁLISIS DEL RIESGO

7.3.1 ANÁLISIS DE CAUSAS

Los objetivos estratégicos y de proceso se desarrollan a través de actividades, pero no todas tienen la misma importancia, por lo tanto, se debe establecer cuáles de ellas contribuyen mayormente al logro de los objetivos y estas son las actividades críticas o factores claves de éxito; estos factores se deben tener en cuenta al identificar las causas que originan la materialización de los riesgos.

Para efectos de esta guía, el análisis de causas se determinará bajo la técnica de lluvia de ideas la cual implica estimular el flujo libre de la conversación entre los responsables con conocimiento de las actividades desarrolladas, de la Entidad, del proceso y del Sistema Integrado de Gestión, para identificar los factores de riesgo, los riesgos, los criterios para la toma de decisiones y las opciones de tratamiento en el plan de manejo de riesgos.

7.3.1.1. Riesgos de seguridad de la información

Tipo de riesgo de seguridad digital o de la información

La clasificación establecida en los tipos de riesgo digital se enfoca de acuerdo con los tres pilares de la seguridad como lo son:

Tipo de riesgo digital	Descripción
Posibilidad de Pérdida de Confidencialidad	Información o recursos privilegiados que son accedidos por personal no autorizado.
Posibilidad de Pérdida de Disponibilidad	Falta de accesibilidad y uso de la información o recursos en una ubicación específica y en el formato correcto.
Posibilidad de Pérdida de Integridad	Ausencia de las características propias relacionadas con la falta o alteración de la información total o parcial. Modificación o borrado de la información.

Tabla 6. *Tipo de riesgo digital*

Tipo de riesgo de bases de datos personales

Tipo de riesgo de bases de datos personales	Descripción
Posibilidad de afectación de la disponibilidad de la plataforma tecnológica, herramientas o aplicativos que gestionan datos personales	Ausencia de medidas que permitan garantizar el acceso oportuno y uso de los datos por parte de las personas interesadas.

Tipo de riesgo de bases de datos personales	Descripción
Posibilidad de pérdida de confidencialidad, divulgación no autorizada o uso inadecuado de la información de datos personales	Los datos personales son divulgados y expuestos a terceros. Son usados para otras finalidades distintas a los cuales fueron autorizadas por el propietario de estos. Se realiza un manejo inadecuado de los datos personales.
Posibilidad de pérdida de integridad, alteración, o modificación de la información de datos personales	Carencia de exactitud de los datos personales debido a la manipulación o modificación de estos ya sea de forma accidental o malintencionada.
Posibilidad de sanciones, quejas, reclamos, solicitudes por incumplimiento de las directrices o normativas frente al tratamiento de los datos personales.	Aplicación de posibles medidas por incumplimiento a la normatividad prevista en la ley 1581 de 2012 y demás que la actualizan y la reglamentan, relacionada con la violación de la confidencialidad, disponibilidad o integridad de los datos personales.

Tabla 7. *Tipo de riesgo de bases de datos personales Fuente: Elaboración propia*

Tipo de Vulnerabilidad

Una vulnerabilidad se refiere a toda aquella debilidad que puede presentar un activo de información, la cual puede ser explotada o usada por intrusos o atacantes comprometiendo la confidencialidad, integridad o disponibilidad de la información.

En el formato F-E-SIG-28 Mapa de riesgos institucional, pestaña riesgos de seguridad de la información, corresponde a la **columna J**, es un campo con una lista desplegable. Entre los diferentes tipos de vulnerabilidades que se tienen identificadas para los activos de información de la entidad se encuentran entre otros los siguientes:

Tipo de Vulnerabilidad	Descripción
1. Datos Personales	Son debilidades en la protección de información que identifica a individuos, como nombres, direcciones o números de identificación. Estas vulnerabilidades pueden permitir accesos no autorizados o uso indebido de esta información sensible.
2. Hardware	Se refiere a fallos o puntos débiles en los equipos físicos, como computadoras, servidores o dispositivos de red. Estas vulnerabilidades pueden permitir daños físicos, robos o accesos no autorizados a los sistemas.
3. Instalaciones / Infraestructura física	Son debilidades en la seguridad de los espacios físicos donde se encuentran los sistemas informáticos, como edificios o centros de datos. Pueden incluir problemas con el control de acceso, protección contra incendios o desastres naturales.
4. Proceso / Seguridad de la información	Son puntos débiles en los procedimientos y flujos de trabajo de la organización. Estas vulnerabilidades pueden llevar a errores humanos, inconsistencias o brechas de seguridad debido a la falta de controles adecuados.
5. Personal	Se refiere a riesgos asociados con las personas que tienen acceso a los sistemas e información. Pueden incluir falta de capacitación, errores humanos o incluso acciones malintencionadas de empleados o contratistas.

Tipo de Vulnerabilidad	Descripción
6. Sistemas de Información / Servicios	Son debilidades en los sistemas que gestionan y procesan la información, como bases de datos o aplicaciones. Estas vulnerabilidades pueden permitir accesos no autorizados, manipulación de datos o interrupciones del servicio.
7. Software	Se refiere a fallos o debilidades en los programas informáticos, que pueden ser explotados para obtener acceso no autorizado, alterar funcionalidades o causar incorrecto funcionamiento del sistema.
8. Red	Son vulnerabilidades en los métodos y políticas diseñados para proteger la información. Pueden incluir fallos en la implementación de controles de seguridad, políticas inadecuadas o falta de seguimiento de las mejores prácticas de seguridad.
9. Información	Se refiere a debilidades en la protección de los datos en sí, independientemente de su formato o ubicación. Estas vulnerabilidades pueden resultar en la exposición, pérdida o alteración no autorizada de información importante.

Tabla 8. *Clasificación tipos de vulnerabilidades. Fuente: Adaptado de Anexo 4. Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas - MINTIC*

VULNERABILIDAD (CAUSA INMEDIATA ¿Cómo?)

Para la identificación de los riesgos asociados a los activos de información, se han propuesto las siguientes vulnerabilidades comunes que pueden llegar a afectar el funcionamiento directo del activo o alterar las propiedades, características de seguridad de la información, las cuales se encuentran clasificadas por los diferentes tipos identificados. Este campo corresponde a una lista desplegable en la cual se deberá seleccionar las diferentes opciones de acuerdo con los tipos de vulnerabilidades presentes en el activo o grupo de activos de información **columna K**.

Tipo de Vulnerabilidad	Descripción
1. Datos Personales	- Inexistencia o insuficiencia de controles de acceso o verificación periódica para validar que la información no ha sido modificada. - No facilitar o generar mecanismos de acceso a la información en materia de datos personales a los titulares. - Tratar datos personales inadecuados o excesivos, de acuerdo con la necesidad de su recolección. - Insuficiente o inexistente participación de los funcionarios y contratistas en las sesiones de sensibilización y toma de conciencia en materia de Protección de Datos Personales. - Ausencia de controles de acceso, falta de gestión de contraseñas o divulgación de información sin los permisos del propietario o titular. - Ausencia o debilidades para la atención de consultas, reclamos, peticiones de rectificación, actualización y supresión de datos personales. - Falta de controles o medidas para proteger los datos personales. - Utilizar los datos personales para finalidades diferentes a las especificadas en su recolección. - Ausencia o carencia de personal que se encargue de la adecuada gestión y tratamiento de los datos personales. - Inexistencia o insuficiencia de copias de respaldo en la nube, o file server de la información de datos personales.

Tipo de Vulnerabilidad	Descripción
	- Fallas en la plataforma tecnológica o herramientas utilizadas para el tratamiento de datos personales. - Inexistencia o insuficiencia de la autorización y soportes para cumplir con la responsabilidad demostrada, en la cual el titular autorizó el tratamiento de los datos personales. - Inexistencia o insuficiencia de identificación, actualización, inhabilitación y reporte de las bases de datos personales, requeridas para cumplir con las funciones de los procesos, dependencias o grupos de trabajo. - Recolectar datos personales inadecuados y/o excesivos para la finalidad del tratamiento. - Inexistencia o insuficiencia de reporte de incidentes de seguridad relacionados con las bases de datos personales en mesa de ayuda. - Conservar los datos personales por periodos de tiempo excesivos cuando ya no se requieren
2. Hardware	- Mantenimiento insuficiente/instalación fallida de los medios de almacenamiento. - Planificación insuficiente del reemplazo de cualquier tipo de hardware o equipo - Susceptibilidad a la humedad, el polvo y la suciedad. - Sensibilidad a la radiación electromagnética - Ausencia de una eficiente gestión de cambios en la configuración - Susceptibilidad a las variaciones de voltaje - Susceptibilidad a las variaciones de temperatura - Almacenamiento sin protección física - Falta de cuidado en la disposición final - Inexistencia o insuficiencia de control de los activos que se encuentran fuera de las instalaciones - Copia no controlada
3. Instalaciones / Infraestructura física	- Uso inadecuado o descuidado del control de acceso físico a edificios, salas y demás recintos. - Ubicación en un área, zona susceptible de inundación - Red de energía inestable - Protección física inexistente o insuficiente de la edificación, puertas, ventanas, rejas, vigilancia. - Inexistencia o insuficiencia de controles de extinción de fuego
4. Proceso / Seguridad de la información	- Ausencia de procedimiento formal para el registro y cancelación de usuarios o su aplicación es ineficaz. - Ausencia de proceso formal para la revisión (supervisión) de los privilegios de acceso o su aplicación es ineficaz. - Ausencia o insuficiencia de políticas, lineamientos, cláusulas (en materia de seguridad) en los contratos con los contratistas, proveedores o terceras partes. - Inexistencia o insuficiencia de procedimientos y controles de monitoreo de los recursos de infraestructura tecnológica para el procesamiento de información - Ausencia de auditorías (supervisiones) no se realizan con regularidad - Ausencia de procedimientos de identificación y gestión de riesgos o su aplicación es ineficaz - Inexistencia o insuficiencia de planificación o ejecución de mantenimiento de los servicios, sistemas de información y aplicativos - Inexistencia o insuficiencia de acuerdos de nivel de servicio - Inexistencia o insuficiencia de procedimiento de gestión de cambios o su aplicación es ineficaz - Ausencia de procedimientos o documentación del SGSI - Inexistencia o insuficiencia de procedimiento formal para la gestión de la información pública, clasificada y reservada o su aplicación es ineficaz - Ausencia de asignación de responsabilidades en materia de seguridad de la información - Inexistencia o insuficiencia de planes de continuidad, están incompletos u obsoletos

Tipo de Vulnerabilidad	Descripción
	- Inexistencia o insuficiencia de políticas específicas de seguridad de la información o su aplicación es ineficaz - Ausencia de procedimientos para la instalación del software en los sistemas operativos - Las responsabilidades en materia de seguridad de la información no están presentes en los contratos de prestación de servicios o nombramientos - No se ha definido el proceso disciplinario en caso de incumplimiento de las políticas o incidentes de seguridad de la información - Inexistencia o insuficiencia de una política de escritorio y de pantalla limpios o su aplicación es ineficaz - Inexistencia o insuficiencia de controles de autorización y acceso a los centros de procesamiento de información física o digital - Inexistencia o insuficiencia de identificación de debilidades de seguridad o monitoreo y gestión de estas - Inexistencia o insuficiencia de procedimientos en materia de derechos de propiedad intelectual o su aplicación es ineficaz
5. Personal	- Ausencia del personal - Procedimientos inadecuados de contratación - Sensibilización y toma de conciencia insuficiente en seguridad de la información - Uso incorrecto de software y hardware - Inexistentes o insuficientes mecanismos o controles de monitoreo - Trabajo de personal externo o de limpieza sin supervisión - Ausencia o desconocimiento de las políticas para el buen uso de los activos (equipos de cómputo, correo electrónico y herramientas colaborativas, internet, información) - Desconocimiento del marco legal y regulatorio, políticas, procedimientos, tratamiento de los datos personales o controles de Seguridad de la Información aplicables a los activos de información. - Falta de reporte de eventos o incidentes de Seguridad de la Información.
6. Sistemas de Información / Servicios	- Asignación errada de privilegios o derechos de acceso - Inexistencia o insuficiencia de alertas de monitoreo o de los servicios y sistemas de información - Configuraciones por defecto o sin cumplir con los requisitos mínimos de seguridad - Inexistencia o insuficiencia de mecanismos de identificación y autenticación de usuario en los sistemas de información o servicios - Daño, modificación, o pérdida de integridad de la información - Insuficiencia o inexistencia de controles de protección contra códigos maliciosos - Incapacidad del sistema o servicio para atender un alto volumen de transacciones, lentitud, degradación del servicio - Insuficiencia o inexistencia de documentación, configuraciones o actualizaciones - Insuficiencia o inexistencia de controles para evitar la intercepción o captura de información - Inexistencia o insuficiencia de copias de respaldo - Inexistencia o insuficiencia de recursos de almacenamiento y procesamiento. - Ausencia o insuficiencia de pruebas de vulnerabilidades - Indisponibilidad, falla o intermitencia de los servicios - Insuficiente o inexistente gestión de contraseñas - Insuficiente o inexistente gestión de soporte y mantenimiento - Punto único de falla

Tipo de Vulnerabilidad	Descripción
7. Software	- Ausencia o insuficiencia de pruebas de software - Vulnerabilidades o desactualizaciones en el software - Ausencia de "bloqueo o cierre de la sesión de usuario" cuando se deja la estación de trabajo - Disposición o reutilización de los medios de almacenamiento sin borrado adecuado de la información - Configuración insuficiente de los registros o logs para fines de auditoria - Asignación errónea de los privilegios de acceso - Interfaz de usuario compleja - Documentación insuficiente o inexistente - Configuración incorrecta de parámetros - Fechas y horas incorrectas - Mecanismos insuficientes o inexistentes de identificación y autentificación, como el Loguin de usuarios - Tablas de contraseñas desprotegidas o en texto claro - Gestión deficiente de las contraseñas - Activación de servicios innecesarios - Software, aplicaciones o sistemas de información nuevos o inmaduros - Especificaciones poco claras o incompletas para los desarrolladores - Inexistencia o insuficiencia de la gestión de cambios - Descarga y uso de programas informáticos no controlados o autorizados - Inexistencia o insuficiencia de copias de respaldo
8. Red	- Ausencia de procedimiento formal para el registro y cancelación de usuarios o su aplicación es ineficaz. - Ausencia de proceso formal para la revisión (supervisión) de los privilegios de acceso o su aplicación es ineficaz. - Ausencia o insuficiencia de políticas, lineamientos, cláusulas (en materia de seguridad) en los contratos con los contratistas, proveedores o terceras partes. - Inexistencia o insuficiencia de procedimientos y controles de monitoreo de los recursos de infraestructura tecnológica para el procesamiento de información - Ausencia de auditorías (supervisiones) no se realizan con regularidad - Ausencia de procedimientos de identificación y gestión de riesgos o su aplicación es ineficaz - Inexistencia o insuficiencia de planificación o ejecución de mantenimiento de los servicios, sistemas de información y aplicativos - Inexistencia o insuficiencia de acuerdos de nivel de servicio - Inexistencia o insuficiencia de procedimiento de gestión de cambios o su aplicación es ineficaz - Ausencia de procedimientos o documentación del SGSI - Inexistencia o insuficiencia de procedimiento formal para la gestión de la información pública, clasificada y reservada o su aplicación es ineficaz - Ausencia de asignación de responsabilidades en materia de seguridad de la información - Inexistencia o insuficiencia de planes de continuidad, están incompletos u obsoletos - Inexistencia o insuficiencia de políticas específicas de seguridad de la información o su aplicación es ineficaz - Ausencia de procedimientos para la instalación del software en los sistemas operativos - Las responsabilidades en materia de seguridad de la información no están presentes en los contratos de prestación de servicios o nombramientos - No se ha definido el proceso disciplinario en caso de incumplimiento de las políticas o incidentes de

Tipo de Vulnerabilidad	Descripción
	seguridad de la información - Inexistencia o insuficiencia de una política de escritorio y de pantalla limpios o su aplicación es ineficaz - Inexistencia o insuficiencia de controles de autorización y acceso a los centros de procesamiento de información física o digital - Inexistencia o insuficiencia de identificación de debilidades de seguridad o monitoreo y gestión de estas - Inexistencia o insuficiencia de procedimientos en materia de derechos de propiedad intelectual o su aplicación es ineficaz
9. Información	- Insuficiencia o inexistencia de revisión y actualización de los controles de acceso a la información física o digital. - Inexistencia o insuficiencia de documentación de procesos, procedimientos, manuales, guías, formatos, otros - Divulgación de información, acceso a información clasificada o reservada - Ingeniería social - Suplantación de identidad - Uso no autorizado de la información - Modificación o alteración no autorizada de la información - Indisponibilidad, pérdida, robo de la información física o digital. - Inexistencia o insuficiencia de acuerdos de confidencialidad - Devolución de activos de información (información física o digital) - Divulgación de información, fuga de información - Incumplimiento de derechos de propiedad intelectual - Retraso en la entrega de información - Destrucción voluntaria o involuntaria de la información física o digital - Reprocesos en la aprobación, oficialización o publicación de información - Ataques cibernéticos, cifrado de información no autorizado, virus, malware

Tabla 9. *Vulnerabilidades comunes Fuente: Adaptado de Anexo 4. Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas – MINTIC*

AMENAZA (CAUSA RAÍZ ¿Por qué?)

Se considera como amenaza (causa) cualquier agente externo al activo que puede aprovechar una vulnerabilidad de este para causar daño y que afectará la seguridad de la información. La identificación de amenazas se realiza mediante la evaluación de fuentes de información como:

- Criterio de expertos: Experiencia de los dueños, propietarios o equipo interdisciplinario que realiza la gestión de riesgo de los activos que se están evaluando.
- Bases de datos públicas sobre amenazas de seguridad de la información.

A continuación, se listan las posibles amenazas que pueden afectar los activos de información de acuerdo con su clasificación y origen. Este campo corresponde a una lista desplegable y se seleccionan los campos de acuerdo con las vulnerabilidades seleccionadas en el campo anterior.

Tipo de Vulnerabilidad	Descripción
1. Datos Personales	- Manipulación o modificación no autorizada de la información de datos personales. - Desconocimiento de normatividad, lineamientos y medios para la atención de consultas, reclamos, peticiones de rectificación, actualización y supresión de datos personales. - Desconocimiento de la normatividad, lineamientos o de la política de protección y tratamiento de datos personales. - Incumplimiento en el tratamiento de los datos personales por parte de los funcionarios, contratistas o terceros. - Divulgación, conocimiento o acceso no autorizado a la información de datos personales - Sanciones, quejas, reclamos frente al tratamiento de los datos personales. - Intrusión informática, manipulación, modificación, eliminación, robo o cifrado de la información de datos personales. - Incumplimiento normativo de la ley de protección de datos personales o de la política de protección y tratamiento de datos personales. - Incumplimiento en el tratamiento, transmisión y/o transferencia de datos personales internamente o con terceros. - Pérdida, modificación o eliminación de datos personales. - Incumplimiento en la atención de PQRS, indisponibilidad de la información - Multas, sanciones, demandas, quejas, reclamos. - Multas, sanciones, demandas, quejas, reclamos. - Incumplimiento normativo de la ley de protección de datos personales o de la política de protección y tratamiento de datos personales. - Multas, sanciones, demandas, quejas, reclamos, investigaciones disciplinarias, incumplimiento normativo de la ley de protección de datos personales - Multas, sanciones, demandas, quejas, reclamos, incumplimiento normativo de la ley de protección de datos personales
2. Hardware	- Incumplimiento en la programación o ejecución de los mantenimientos - Destrucción o daño de equipos o de medios. - Polvo, corrosión, congelamiento, líquidos - Radiación electromagnética - Error en el uso, afectación del servicio - Pérdida del suministro de energía, indisponibilidad de los equipos de suministro energético redundantes - Fenómenos meteorológicos, daños del aire acondicionado - Hurto de medios o documentos - Hurto de medios o equipos, pérdida o divulgación de información - Hurto de equipo - Hurto, pérdida o divulgación de información
3. Instalaciones / Infraestructura física	- Destrucción de equipo o medios - Inundación - Pérdida del suministro de energía - Hurto de equipo - Incendios

Tipo de Vulnerabilidad	Descripción
4. Proceso / Seguridad de la información	- Abuso de los privilegios de acceso - Abuso de los privilegios de acceso - Abuso de los privilegios de acceso - Indisponibilidad de los servicios por tiempos prolongados - Abuso de los privilegios de acceso - Abuso de los privilegios de acceso - Incumplimiento en el mantenimiento de los servicios, sistemas de información y aplicativos - Indisponibilidad de los servicios por tiempos prolongados - Incumplimiento en el mantenimiento del sistema de información - Incumplimiento normativo interno o externo - Incumplimiento normativo interno o externo - Negación de acciones, incumplimiento normativo interno o externo - Indisponibilidad de los servicios por tiempos prolongados - Pérdida de disponibilidad, integridad o confidencialidad - Error en el uso, derechos de autor, incumplimiento en el licenciamiento - Negación de acciones, incumplimiento normativo interno o externo - Negación de acciones, incumplimiento normativo interno o externo - Hurto de medios o documentos - Hurto de medios o documentos - Hurto de medios o documentos, negación de acciones, incumplimiento normativo interno o externo, investigaciones disciplinarias - Uso de software falso o copiado, incumplimiento normativo interno o externo
5. Personal	- Incumplimiento en la disponibilidad del personal - Destrucción de equipos o medios - Error en el uso - Error en el uso - Procesamiento ilegal de los datos - Hurto de medios o documentos - Uso no autorizado del equipo - Multas, sanciones, demandas, quejas, reclamos, investigaciones disciplinarias - Ataques cibernéticos, pérdida, modificación, divulgación de información, desinformación, indisponibilidad de los servicios
6. Sistemas de Información / Servicios	- Acceso no autorizado, errores humanos - Degradación, denegación de servicio, indisponibilidad - Ataque informático, ingeniería social - Suplantación de usuarios - Ataques informáticos, errores humanos - Ataques informáticos, errores humanos - Indisponibilidad de los sistemas de información o servicios por tiempos prolongados, denegación de servicios - Indisponibilidad de los servicios por tiempos prolongados - Ataque informático, correos maliciosos, errores humanos

Tipo de Vulnerabilidad	Descripción
	- Falla de herramientas o medios - Errores humanos, falta de monitoreo - Acceso no autorizado, ataque informático, configuraciones por defecto - Fallas de infraestructura tecnológica - Acceso no autorizado, phishing - Errores humanos, indisponibilidad por tiempos prolongados - Falla de equipos
7. Software	- Abuso de los privilegios de acceso, pérdida o divulgación de información, pérdida de integridad - Indisponibilidad de los servicios, materialización de incidentes - Abuso de los privilegios de acceso, pérdida o divulgación de información, pérdida de integridad - Acceso no autorizado, divulgación de información - Abuso de los privilegios de acceso, pérdida de integridad de la información, imposibilidad de rastreo de acciones - Abuso de los privilegios de acceso - Error en el uso - Error en el uso - Error en el uso - Error en el uso, pérdida de integridad de la información - Suplantación de identidad, abuso de los privilegios de acceso, acceso no autorizado - Suplantación de identidad, abuso de los privilegios de acceso, acceso no autorizado - Suplantación de identidad, abuso de los privilegios de acceso, acceso no autorizado - Procesamiento no autorizado de datos - Mal funcionamiento del software - Mal funcionamiento del software, retrasos o incumplimientos - Mal funcionamiento, indisponibilidad prolongada del software - Ciberataques, pérdida de información, incumplimiento de los derechos de propiedad intelectual - Indisponibilidad prolongada de los servicios y pérdida de información
8. Red	- Abuso de los privilegios de acceso - Abuso de los privilegios de acceso - Abuso de los privilegios de acceso - Indisponibilidad de los servicios por tiempos prolongados - Abuso de los privilegios de acceso - Abuso de los privilegios de acceso - Incumplimiento en el mantenimiento de los servicios, sistemas de información y aplicativos - Indisponibilidad de los servicios por tiempos prolongados - Incumplimiento en el mantenimiento del sistema de información - Incumplimiento normativo interno o externo - Incumplimiento normativo interno o externo - Negación de acciones, incumplimiento normativo interno o externo - Indisponibilidad de los servicios por tiempos prolongados - Pérdida de disponibilidad, integridad o confidencialidad - Error en el uso, derechos de autor, incumplimiento en el licenciamiento

Tipo de Vulnerabilidad	Descripción
	- Negación de acciones, incumplimiento normativo interno o externo - Negación de acciones, incumplimiento normativo interno o externo - Hurto de medios o documentos - Hurto de medios o documentos - Hurto de medios o documentos, negación de acciones, incumplimiento normativo interno o externo, investigaciones disciplinarias - Uso de software falso o copiado, incumplimiento normativo interno o externo
9. Información	- Acceso no autorizado, elevación de privilegios - Insuficiencia o ausencia de personal - Errores humanos, acceso no autorizado - Errores humanos, desconocimiento tecnológico, acceso no autorizado - Phishing, malware, contraseñas débiles - Errores humanos, acceso no autorizado - Errores humanos, acceso no autorizado, elevación de privilegios - Caída de servicios, fallas tecnológicas, daño e inaccesibilidad en edificaciones o archivos, ausencia de copias de respaldo - Incumplimiento normativo interno o externo - Terminación o cambio de empleo - Inexistencia o insuficiencia de controles en actividades de Teletrabajo o trabajo remoto. - Incumplimiento normativo interno o externo - Insuficiencia o ausencia de personal, errores humanos - Humedad, polvo, incendio, inundación, errores humanos - Incumplimiento normativo interno o externo, errores humanos - Inexistencia o insuficiencia de controles de acceso, contraseñas débiles, errores humanos

Tabla 10. *Amenazas comunes Fuente: Adaptado de Anexo 4. Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas – MINTIC*

Consecuencia (lo que podría afectar o generar)

Efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas. A continuación, en la **columna O**, se listan las consecuencias identificadas para la evaluación de los riesgos de seguridad de la información:

Consecuencias
Acceso de la información por parte de personal no autorizado
Accesos no autorizados en instalaciones físicas (Centro de cómputo, cableado, edificios, entre otros)
Daños de imagen, reputación y buen nombre del proceso o institucional
Demoras en la prestación de los servicios de información, misionales o tecnológicos
Demoras en los procesos administrativos institucionales para el desarrollo de su gestión
Falla (s) en el funcionamiento de los sistemas de información
Incumplimiento Ley de protección de datos personales y Hábeas Data.

Consecuencias
Incumplimientos legales o normativos
Indisponibilidad de la información institucional a los usuarios
Investigaciones, hallazgos y posibles sanciones de los Entes de control internos y externos
Pérdida o eliminación de la información
Pérdida parcial o total de información física o digital
Pérdidas económicas
Publicación de datos personales o confidenciales
Quejas y reclamos de los usuarios
Reprocesos administrativos o financieros para intentar restaurar la información
Reprocesos, demoras y paralizaciones en la ejecución de actividades
Robo de datos y equipos
Suplantación de la identidad
Toma de decisiones inadecuadas

Tabla 11. *Lista de consecuencias Fuente: Adaptado de Guía de Gestión de Riesgos – MINTIC*

7.3.2 DETERMINAR LA PROBABILIDAD

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

Para su determinación se utiliza la Tabla 12. Criterios para calificar la probabilidad de los **riesgos de gestión, ambientales y fiscales**

	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%**

Tabla 12. *Criterios para calificar la probabilidad- riesgos de gestión, ambientales y fiscales. Fuente: DAFP. 2022.*

Nota: Si la actividad es permanente calificar la frecuencia de la actividad como muy alta y en frecuencia colocar un valor superior a 5000 veces por año.

Para los riesgos de **seguridad de la información,** su determinación se utiliza la Tabla 13. Criterios para calificar la probabilidad de riesgos de Seguridad de la Información

	Frecuencia de la actividad	Probabilidad
Muy baja	La actividad que conlleva el riesgo se ejecuta como máximo **5** veces por año	**20%**
Baja	La actividad que conlleva el riesgo se ejecuta de **6** a **25** veces por año	**40%**
Media	La actividad que conlleva el riesgo se ejecuta de **26** a **150** veces por año	**60%**
Alta	La actividad que conlleva el riesgo se ejecuta de **151** a **300** veces por año	**80%**
Muy Alta	La actividad que conlleva el riesgo se ejecuta más de **301** veces por año	**100%**

Tabla 13. *Criterios para calificar la probabilidad de riesgos de Seguridad de la Información. Fuente: Adaptado DAFP 2022*

Para la gestión de **riesgos de corrupción**, continúan vigentes los lineamientos contenidos en la versión 4 de la Guía para la administración del riesgo y el diseño de controles en entidades públicas de 2018. Para dichos riesgos por probabilidad se entiende la posibilidad de ocurrencia del riesgo, ésta puede ser medida con criterios de frecuencia o factibilidad.

Bajo el criterio de frecuencia se analizan el número de eventos en un periodo determinado, se trata de hechos que se han materializado o se cuenta con un historial de situaciones o eventos asociados al riesgo.

Bajo el criterio de factibilidad se analiza la presencia de factores internos y externos que pueden proporcionar el riesgo, se trata en este caso de un hecho que no se ha presentado, pero es posible que se dé.

Para su determinación se utiliza la Tabla 14. Criterios para calificar la probabilidad riesgos de corrupción

Nivel	Probabilidad	Descripción (factibilidad)	Frecuencia
1	Rara vez	El evento puede ocurrir solo en circunstancias excepcionales. (poco comunes o anormales)	No se ha presentado en los últimos 5 años.
2	Improbable	El evento puede ocurrir en algún momento.	Al menos 1 vez en los últimos 5 años.
3	Posible	El evento podrá 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.

Tabla 14. *Criterios para calificar la probabilidad- riesgos de corrupción. Fuente: DAFP. 2018.*

En caso de que no se cuente con datos históricos sobre el número de eventos que se hayan materializado en un periodo de tiempo, los integrantes del equipo de trabajo deben calificar en privado el nivel de probabilidad en términos de factibilidad, utilizando la siguiente matriz de priorización de probabilidad.

N°	RIESGO	P1	P2	P3	P4	P5	P6	TOT	PROM	
1	Inoportunidad en la adquisición de los bienes y servicios requeridos por la entidad	Se espera que el evento ocurra en la mayoría de las circunstancias.	5	4	3	5	3	24	4	4 PROBABLE
2	Otros riesgos identificados	Es viable que el evento ocurra en la mayoría de las circunstancias.								
3	Otros riesgos	El evento podrá ocurrir en algún momento.								

Convenciones:

N.°: número consecutivo del riesgo - **P1**: participante 1 P… - **Tot**: total puntaje - **Prom**.: promedio

Tabla 15. *Matriz de priorización de probabilidad- riesgos de corrupción. Fuente: DAFP. 2018.*

7.3.3 DETERMINAR EL IMPACTO

Para la construcción de la tabla de criterios se definen los impactos económicos y reputacionales como las variables principales.

Cuando se presenten ambos impactos para un riesgo, tanto económico como reputacional, con diferentes niveles se debe tomar el nivel más alto, así, por ejemplo: para un riesgo identificado se define un impacto económico en nivel insignificante e impacto reputacional en nivel moderado, se tomará el más alto, en este caso sería el nivel moderado.

Para su determinación se utiliza la Tabla 16. Criterios para definir el nivel de impacto de los **riesgos de gestión, ambientales y fiscales**

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

Tabla 16. *Criterios para definir el nivel de impacto - riesgos de gestión, ambientales y fiscales. Fuente: DAFP. 2022.*

Para los riesgos de **seguridad de la información,** su determinación se utiliza la Tabla 17. *Criterios para definir el nivel de impacto - riesgos de seguridad de la información:*

	Afectación económica	Afectación Reputacional
Leve 20%	Pérdida económica hasta 10 SMLMV	El riesgo afecta la imagen de algún área de la organización.
Menor 40%	Pérdida económica de 11 hasta 20 SMLMV	El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, de junta directiva y accionistas y/o de proveedores.
Moderado 60%	Pérdida económica de 21 hasta 100 SMLMV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos.
Mayor 80%	Pérdida económica de 101 hasta 500 SMLMV	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector.
Catastrófico 100%	Pérdida económica superior a 501 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país.

Tabla 17. *Criterios para calificar el impacto de riesgos de Seguridad de la Información. Fuente: Adaptado DAFP 2022*

	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%**

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

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

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

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

Diagrama 6. *Ejemplo aplicado a tablas de probabilidad e impacto. Fuente: Guía para la Administración del Riesgo y el Diseño de Controles en entidades Públicas-DAFP. 2020.*

Para la adecuada calificación de **riesgos de seguridad de la información** se debe tener en cuenta lo siguiente:

- Las variables confidencialidad, integridad y disponibilidad se definen de acuerdo con el modelo de seguridad y privacidad de la información de la estrategia de Gobierno Digital (GD) del Ministerio de Tecnologías de la Información y las Comunicaciones.
- La variable población se define teniendo en cuenta el establecimiento del contexto externo de la entidad, es decir, que la consideración de población va a estar asociada a las personas a las cuales se les prestan servicios o trámites en el entorno digital y que de una u otra forma pueden verse afectadas por la materialización de algún riesgo en los activos identificados.
  Los porcentajes en las escalas pueden variar, según la entidad y su contexto.
- La variable presupuesto es la consideración de presupuesto afectado por la entidad debido a la materialización del riesgo, contempla sanciones económicas o impactos directos en la ejecución presupuestal.
- La variable ambiental estará también alineada con la afectación del medio ambiente por la materialización de un riesgo de seguridad digital. Esta variable puede no ser utilizada en la mayoría de los casos, pero debe tenerse en cuenta, ya que en alguna eventualidad puede existir afectación ambiental.

Para la determinación del nivel de impacto o consecuencias de los **riesgos de corrupción** se utiliza la Tabla 18. Criterios para calificar el impacto - riesgos de corrupción.

Formato para determinar el impacto			
No	**Pregunta**	**Respuesta**	
	Si el riesgo de corrupción se materializa podría…	**Si**	**No**
1	Afectar al grupo de funcionarios del proceso		
2	Afectar el cumplimiento de metas y objetivos de la dependencia		
3	Afectar el cumplimiento de la misión de la entidad		
4	Afectar el cumplimiento de la misión del sector a la que pertenece la entidad		
5	Generar pérdida de confianza de la entidad, afectando su reputación		
6	Generar pérdida de recursos económicos		
7	Afectar la generación de los productos o la prestación de servicios de la entidad		
8	Dar lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien o servicios o los recursos públicos		
9	Generar pérdida de información de la entidad		
10	Generar intervención de los órganos de control, de la fiscalía, u otro ente		
11	Dar lugar a proceso sancionatorios		
12	Dar lugar a procesos disciplinarios		

Formato para determinar el impacto			
No	**Pregunta**	**Respuesta**	
	Si el riesgo de corrupción se materializa podría…	**Si**	**No**
13	Dar lugar a procesos fiscales		
14	Dar lugar a procesos penales		
15	Generar pérdida de credibilidad del sector		
16	Ocasionar lesiones físicas o pérdida de vidas humanas		
17	Afectar la imagen regional		
18	Afectar la imagen nacional		
19	Generar daño ambiental		

Tabla 18. *Criterios para calificar el impacto - riesgos de corrupción. Fuente: DAFP. 2020.*

Por lo anterior, y teniendo en cuenta las respuestas a las preguntas referentes a la valoración de los riesgos de corrupción se establece la siguiente valoración:

Nivel	Impacto	Descripción	Riesgos de Corrupción
3	MODERADO	Si el hecho llegara a presentarse, tendría medianas consecuencias o efectos sobre la entidad y el proceso.	Responder afirmativamente de UNO a CINCO preguntas(s) genera un impacto MODERADO
4	MAYOR	Si el hecho llegara a presentarse, tendría altas consecuencias o efectos sobre la entidad y el proceso.	Responder afirmativamente de SEIS a ONCE preguntas genera un impacto MAYOR
5	CATASTRÓFICO	Si el hecho llegara a presentarse, tendría desastrosas consecuencias o efectos sobre la entidad y el proceso.	Responder afirmativamente de DOCE a DIECINUEVE preguntas genera un impacto CATASTRÓFICO

Tabla 19. *Criterios para calificar el impacto - riesgos de corrupción. Fuente: DAFP.2020*

Tratándose de **riesgos de corrupción** el impacto siempre será negativo; en este orden de ideas no aplica la descripción de riesgos leves o menores.

7.4 EVALUACIÓN DEL RIESGO

7.4.1 ESTIMAR EL NIVEL DEL RIESGO INICIAL (RIESGO INHERENTE)

Se logra a través de la determinación de la probabilidad y el impacto como se mencionó anteriormente por medio de las tablas establecidas. Para su determinación se utiliza la Matriz de criticidad de 5x5, la cual determina que para ubicar el nivel de riesgo se cuenta con cinco niveles en probabilidad y 5 niveles en impacto, Se definen 4 zonas de severidad en la matriz de calor, como se muestra a continuación:

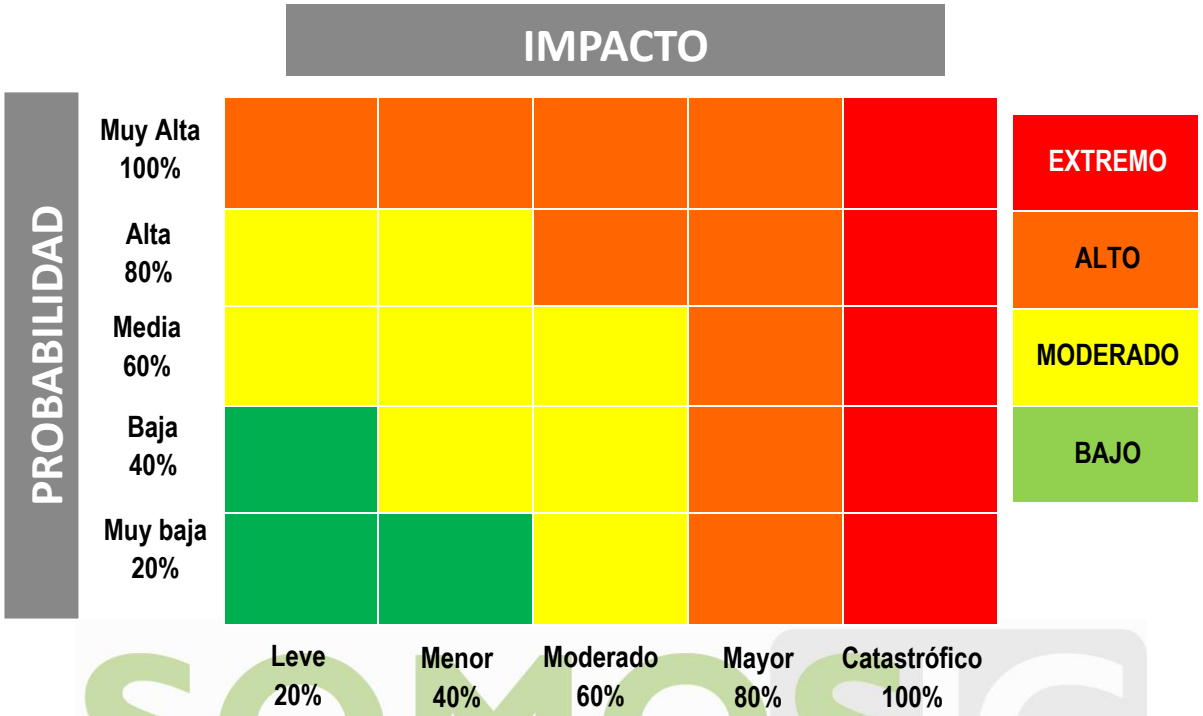


Diagrama 7. *Matriz de calor (niveles de severidad del riesgo) riesgos de gestión, ambientales, de seguridad de la información y fiscales. Fuente: Guía para la Administración del Riesgo y el Diseño de Controles en entidades Públicas - DAFP. 2022.*

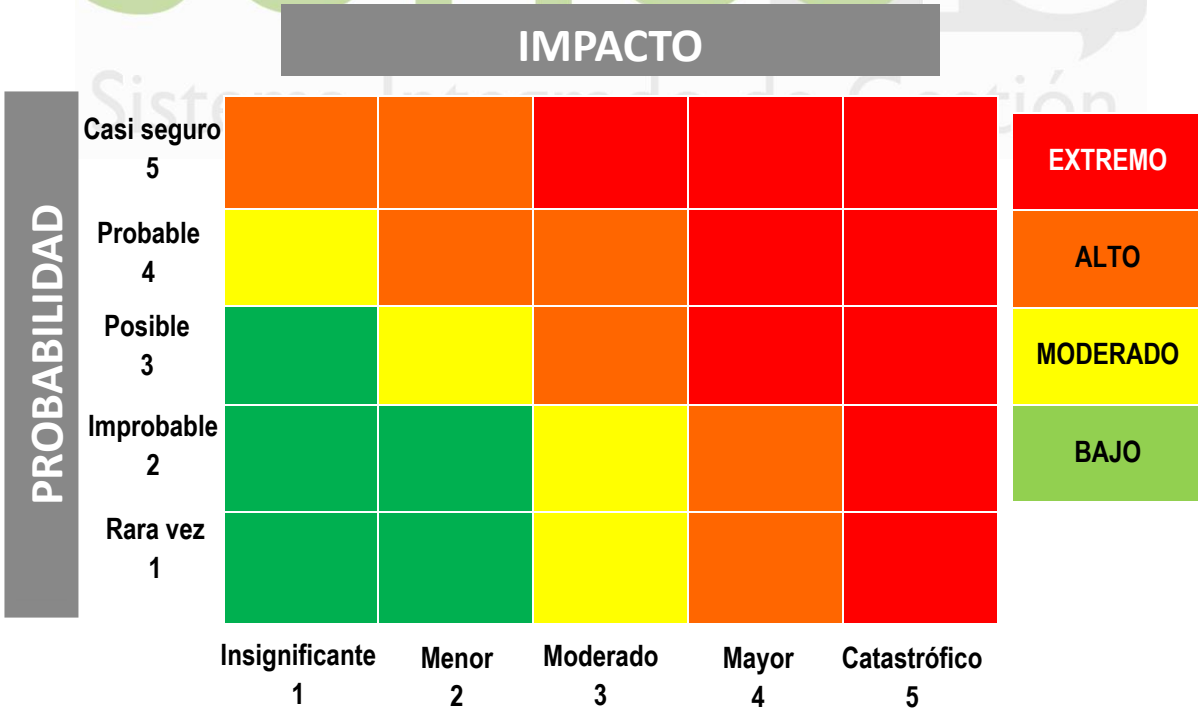


Diagrama 8. *Matriz de calor (niveles de severidad del riesgo) riesgos de corrupción. Fuente: Guía para la Administración del Riesgo y el Diseño de Controles en entidades Públicas - DAFP. 2018.*

El mapa de calor permite visualizar los riesgos en las zonas definidas (bajo, moderado, alto y extremo) permitiendo identificar y priorizar los riesgos asociados a su gestión que requieren mayor atención, así como los que está dispuesta a aceptar en función del impacto de estos en la Entidad.

Frente a las zonas de riesgo se define el siguiente tratamiento:

Zona de riesgo Baja: Aceptar el riesgo.
Zona de riesgo Moderada: Reducir el riesgo.
Zona de riesgo Alta: Reducir el riesgo, evitar, transferir o compartir
Zona de riesgo Extrema: Reducir el riesgo, evitar, transferir o compartir

Los riesgos que se encuentren en zona baja se aceptan (**apetito del riesgo**) y se continúa el monitoreo, con el fin de garantizar que las condiciones bajo las cuales han sido analizados no han cambiado, si las condiciones cambian, es necesario volver a valorar y si es el caso determinar el manejo correspondiente a través de los controles que sean necesarios. Así mismo, los riesgos de corrupción **NO** admiten la aceptación del riesgo, siempre deben conducir a un tratamiento.

Los riesgos que se encuentran en las zonas más altas o de mayor gravedad son los que se priorizan disminuyéndose para estos el nivel de aceptación, determinando en el plan de contingencia las actividades de control (correctivas) que ataquen las causas del riesgo, cuando éste se llegue a materializar.

Esto ayuda a la Entidad a mejorar su administración de riesgos, priorizando los esfuerzos y acciones sobre los riesgos potencialmente de mayor impacto.

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

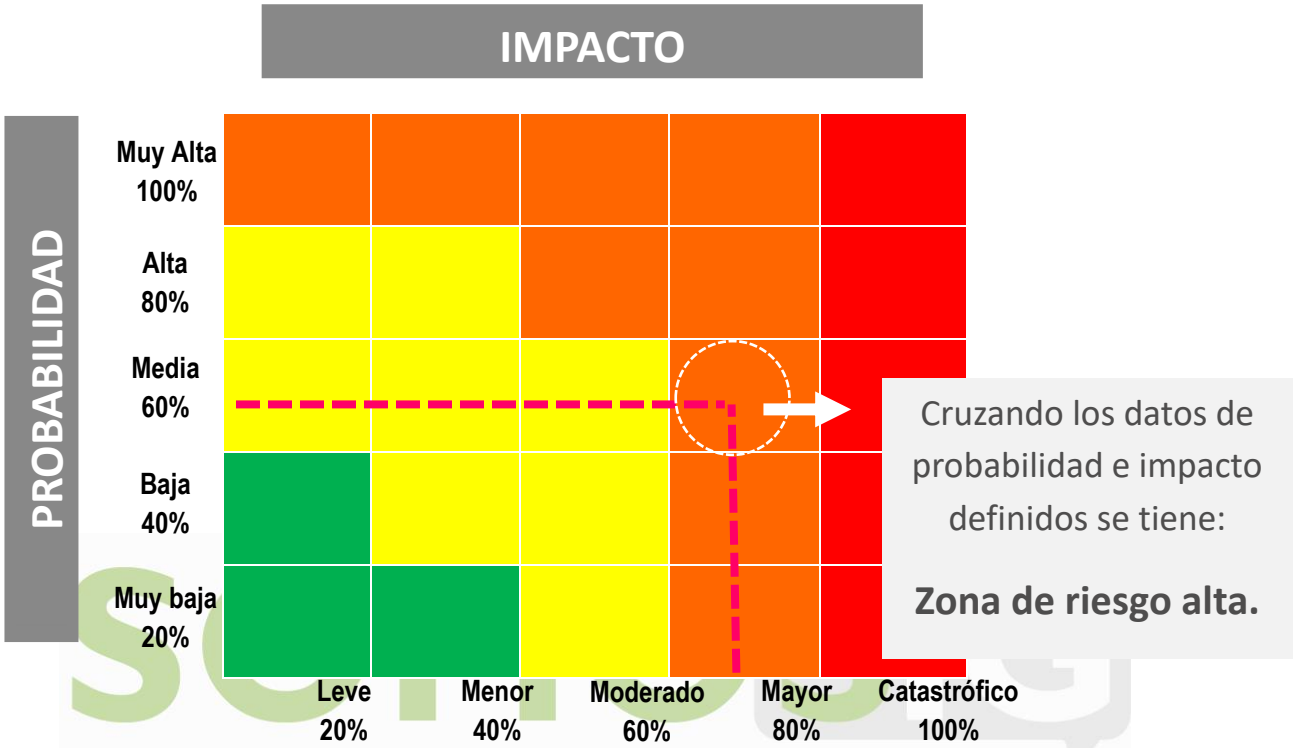


Diagrama 9. *Ejemplo aplicado matriz de calor. Fuente: Guía para la Administración del Riesgo y el Diseño de Controles en entidades Públicas-DAFP. 2020.*

Frente al análisis de probabilidad e impacto no se utiliza criterio experto, esto quiere decir que el líder del proceso, como conocedor de su quehacer, define cuántas veces desarrolla la actividad, esto para el nivel de probabilidad, y es a través de la tabla establecida que se ubica en el nivel correspondiente, dicha situación se repite para el impacto, ya que no se trata de un análisis subjetivo. Se debe señalar que el criterio experto, es decir el conocimiento y experticia del líder del proceso, se utiliza para definir aspectos como: número de veces que se ejecuta la actividad, cadena de valor del proceso, factores generadores y para la definición de los controles.

7.4.2 VALORACIÓN DE CONTROLES

Se busca confrontar los resultados del análisis del riesgo inicial (INHERENTE) frente a los controles establecidos, con el fin de determinar la zona de riesgo final (RESIDUAL).

Riesgo inicial (Inherente) – Efecto de los controles = Riesgo Final (Residual)

Los responsables de implementar y monitorear los controles son los líderes de proceso con el apoyo de su equipo de trabajo.

Al momento de definir las actividades de control por parte de la primera línea de defensa, es importante considerar que los controles estén bien diseñados, es decir, que efectivamente estos mitigan las causas que hacen que el riesgo se materialice.

Para los **riesgos de gestión, ambientales y fiscales,** se realiza de acuerdo con lo descrito a continuación**:**

- Valoración de los controles – diseño de controles

Las actividades de control, independientemente de la tipología de riesgo a tratar, deben tener una adecuada combinación para prevenir que la situación de riesgo se origine. Ahora, en caso de que la situación de riesgos se presente, esta debe ser detectada de manera oportuna, es así, como se encuentra la siguiente clasificación de las actividades de control:

- 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. Va a las causas del riesgo, atacan la probabilidad de ocurrencia del riesgo.

- Control detectivo: control accionado durante la ejecución del proceso. Estos controles detectan el riesgo, pero generan reprocesos. Detecta que algo ocurre y devuelve el proceso a los controles preventivos, atacan la probabilidad de ocurrencia del riesgo.

- Control correctivo: control accionado en la salida del proceso y después de que se materializa el riesgo. Estos controles tienen costos implícitos. Atacan el impacto frente a la materialización del riesgo

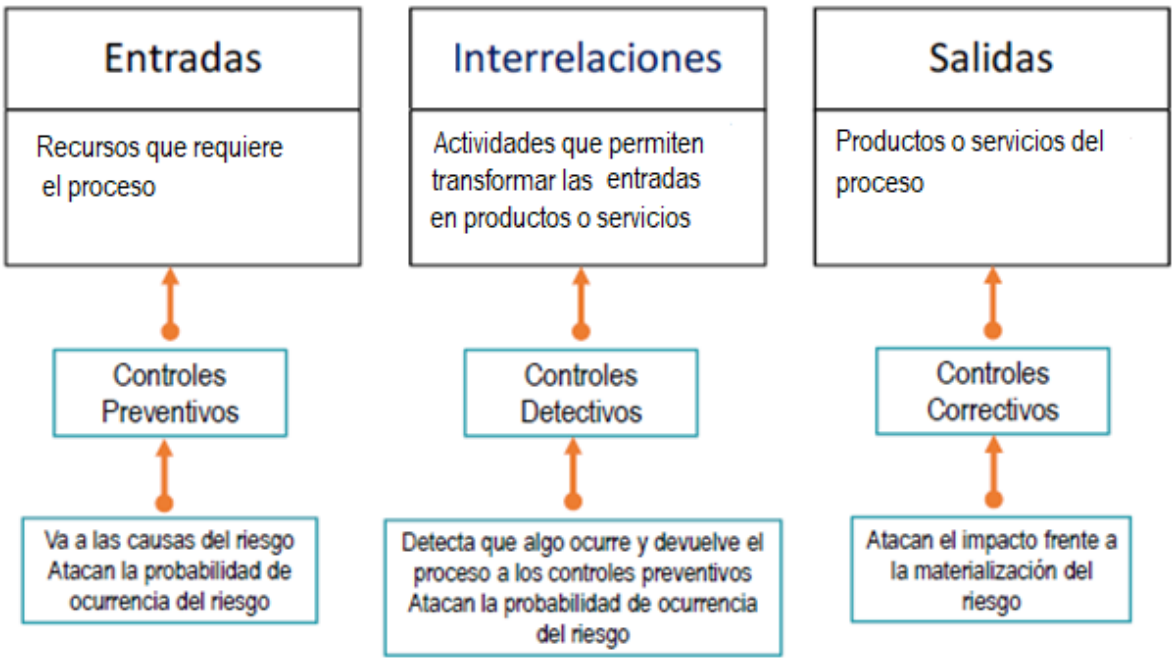


Diagrama 10. *Ciclo del proceso y las tipologías de controles Fuente: Guía para la Administración del Riesgo y el Diseño de Controles en entidades Públicas-DAFP. 2022*

Al momento de definir si un control o los controles mitigan de manera adecuada el riesgo se deben considerar, desde la redacción del mismo, las siguientes variables:

- 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.

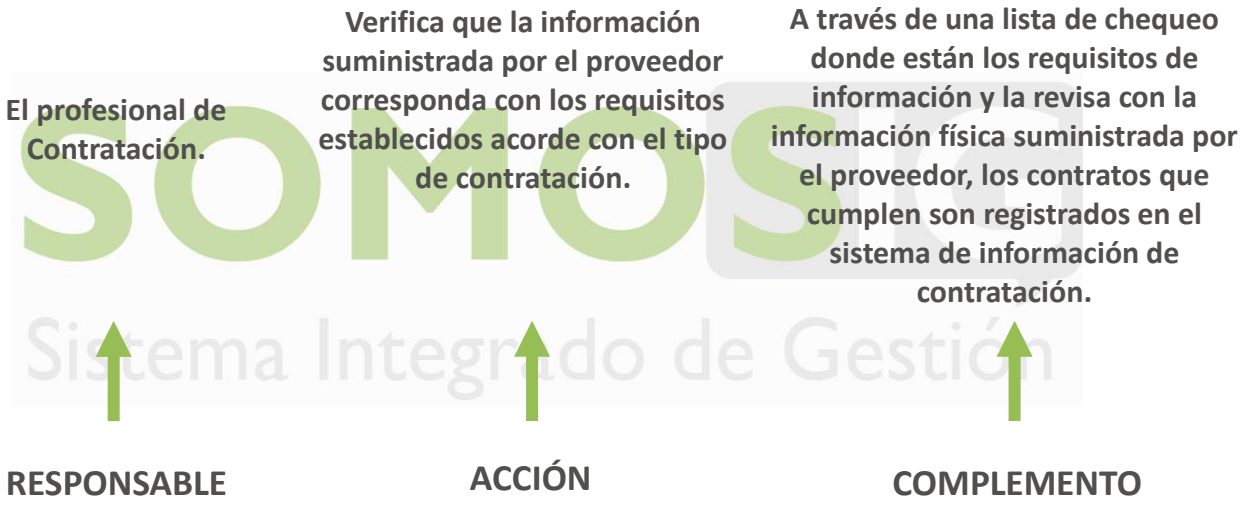


Diagrama 11. *Ejemplo aplicado redacción del control. Fuente: Guía para la Administración del Riesgo y el Diseño de Controles en entidades Públicas-DAFP. 2020.*

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

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

Dominio

Para los riesgos de Seguridad de la Información los dominios en la ISO 27001 corresponden a categorías o áreas temáticas principales de la seguridad de la información. Cada dominio agrupa objetivos de control y controles relacionados, proporcionando una estructura organizativa para los requisitos de seguridad. En este apartado, la información se encuentra organizada con respecto a los 14 dominios definidos en la ISO 27001, abarcando así de manera integral los aspectos clave de la gestión de la seguridad de la información, así:

Dominio
A.5 Políticas de la Seguridad de la Información
A.6 Organización de la Seguridad de la Información
A.7 Seguridad de los Recursos Humanos
A.8 Gestión de Activos
A.9 Control de Acceso
A.10 Criptografía
A.11 Seguridad Física y del Entorno
A.12 Seguridad de las Operaciones
A.13 Seguridad de las Comunicaciones
A.14 Adquisición Mantenimiento y Desarrollo de Sistemas
A.15 Relaciones con los Proveedores
A.16 Gestión de Incidentes de Seguridad de la Información
A.17 Aspectos de Seguridad de la Información de la Gestión de Continuidad de Negocio
A.18 Cumplimiento

Tabla 20 *Lista de dominios anexo A Fuente: ISO 27001*

Controles ISO 27001

Para los riesgos de **Seguridad de la Información** los controles relacionados en este apartado se encuentran alineados con los 114 controles del anexo A de la ISO 27001 y deben considerarse para mitigar las causas que hacen que el riesgo se pueda materializar conforme a las vulnerabilidades identificadas.

Los controles relacionados en este apartado se encuentran alineados con los 114 controles del anexo A de la ISO 27001 y deben considerarse para mitigar las causas que hacen que el riesgo se pueda materializar conforme a las vulnerabilidades identificadas. De igual forma deben considerarse los lineamientos establecidos en el numeral **7.4.2. VALORACION DE CONTROLES** de la G-E-SIG-05 - Guía de administración del riesgo del Ministerio de Ambiente y Desarrollo Sostenible, como se describe a continuación:

Controles	Descripción del control
A.5.1.1-Políticas para la seguridad de la información	Se debería definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y partes externas pertinentes.
A.5.1.2-Revisión de la política de seguridad de la información	Las políticas para seguridad de la información se deberían revisar a intervalos planificados o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continuas.
A.6.1.1-Seguridad de la información roles y responsabilidades	Se deberían definir y asignar todas las responsabilidades de la seguridad de la información.

Controles	Descripción del control
A.6.1.2-Separación de deberes	Los deberes y áreas de responsabilidad en conflicto se deberían separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización.
A.6.1.3-Contacto con las autoridades	Se deberían mantener los contactos apropiados con las autoridades pertinentes.
A.6.1.4-Contacto con grupos de interés especial	Es conveniente mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad.
A.6.1.5-Seguridad de la información en gestión de proyectos	La seguridad de la información se debería tratar en la gestión de proyectos, independientemente del tipo de proyecto.
A.6.2.1-Política para dispositivos móviles	Se deberían adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.
A.6.2.2-Teletrabajo	Se deberían implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.
A.7.1.1-Selección	Las verificaciones de los antecedentes de todos los candidatos a un empleo se deberían llevar a cabo de acuerdo con las leyes, reglamentos y ética pertinentes, y deberían ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos.
A.7.1.2-Términos y condiciones del empleo	Los acuerdos contractuales con empleados y contratistas, deberían establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.
A.7.2.1-Responsabilidades de la dirección	La dirección debería exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.
A.7.2.2-Toma de conciencia, educación y formación en la seguridad de la información	Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deberían recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo.
A.7.2.3-Proceso disciplinario	Se debería contar con un proceso disciplinario formal el cual debería ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.
A.7.3.1-Terminación o cambio de responsabilidades de empleo	Las responsabilidades y los deberes de seguridad de la información que permanecen validos después de la terminación o cambio de contrato se deberían definir, comunicar al empleado o contratista y se deberían hacer cumplir.
A.8.1.1-Inventario de activos	Se deberían identificar los activos asociados con la información y las instalaciones de procesamiento de información, y se debería elaborar y mantener un inventario de estos activos.
A.8.1.2-Propiedad de los activos	Los activos mantenidos en el inventario deberían tener un propietario.

Controles	Descripción del control
A.8.1.3-Uso aceptable de los activos	Se deberían identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.
A.8.1.4-Devolución de activos	Todos los empleados y usuarios de partes externas deberían devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.
A.8.2.1-Clasificación de la información	La información se debería clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.
A.8.2.2-Etiquetado de la información	Se debería desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización
A.8.2.3-Manejo de activos	Se deberían desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.
A.8.3.1-Gestión de medios de soporte removibles	Se deberían implementar procedimientos para la gestión de medios removibles, de acuerdo con el esquema de clasificación adoptado por la organización.
A.8.3.2-Disposición de los medios de soporte	Se debería disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.
A.8.3.3-Transferencia de medios de soporte físicos	Los medios que contienen información se deberían proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.
A.9.1.1-Política de control de acceso	Se debería establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.
A.9.1.2-Acceso a redes y a servicios en red	Solo se debería permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.
A.9.2.1-Registro y cancelación del registro de usuarios	Se debería implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.
A.9.2.2-Suministro de acceso de usuarios	Se debería implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso a todo tipo de usuarios para todos los sistemas y servicios.
A.9.2.3-Gestión de derechos de acceso privilegiado	Se debería restringir y controlar la asignación y uso de derechos de acceso privilegiado.
A.9.2.4-Gestión de información de autenticación secreta de usuarios	La asignación de la información secreta se debería controlar por medio de un proceso de gestión formal.
A.9.2.5-Revisión de los derechos de acceso de usuarios	Los propietarios de los activos deberían revisar los derechos de acceso de los usuarios, a intervalos regulares.

Controles	Descripción del control
A.9.2.6-Retiro o ajuste de los derechos de acceso	Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deberían retirar al terminar su empleo, contrato o acuerdo, o se deberían ajustar cuando se hagan cambios.
A.9.3.1-Uso de información de autenticación secreta	Se debería exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.
A.9.4.1-Restricción de acceso a información	El acceso a la información y a las funciones de los sistemas de las aplicaciones se debería restringir de acuerdo con la política de control de acceso.
A.9.4.2-Procedimiento de ingreso seguro	Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debería controlar mediante un proceso de ingreso seguro.
A.9.4.3-Sistema de gestión de contraseñas	Los sistemas de gestión de contraseñas deberían ser interactivos y deberían asegurar la calidad de las contraseñas.
A.9.4.4-Uso de programas utilitarios privilegiados	Se debería restringir y controlar estrictamente el uso de programas utilitarios que pudieran tener capacidad de anular el sistema y los controles de las aplicaciones
A.9.4.5-Control de acceso a códigos fuente de programas	Se debería restringir el acceso a los códigos fuente de los programas.
A.10.1.1-Política sobre el uso de controles criptográficos	Se debería desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información
A.10.1.2-Gestión de Llaves	Se debería desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas durante todo su ciclo de vida.
A.11.1.1-Perímetro de seguridad física	Se deberían definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información sensible o critica, e instalaciones de manejo de información
A.11.1.2-Controles de acceso físico	Las áreas seguras se deberían proteger mediante controles de entrada apropiados para asegurar que solamente se permite el acceso a personal autorizado.
A.11.1.3-Seguridad de oficinas, recintos e instalaciones	Se debería diseñar y aplicar seguridad física a oficinas, recintos e instalaciones.
A.11.1.4-Protección contra amenazas externas y ambientales	Se debería diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes
A.11.1.5-Trabajo en áreas seguras	Se deberían diseñar y aplicar procedimientos para trabajo en áreas seguras.
A.11.1.6-Áreas de carga, despacho y acceso público	Se deberían controlar los puntos de acceso tales como áreas de despacho y de carga, y otros puntos en donde pueden entrar personas no autorizadas, y si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.
A.11.2.1-Ubicación y protección de los equipos	Los equipos deberían estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las oportunidades para acceso no autorizado.
A.11.2.2-Servicios públicos de soporte	Los equipos se deberían proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.

Controles	Descripción del control
A.11.2.3-Seguridad del cableado	El cableado de potencia y de telecomunicaciones que porta datos o soporta servicios de información debería estar protegido contra interceptación, interferencia o daño
A.11.2.4-Mantenimiento de los equipos	Los equipos se deberían mantener correctamente para asegurar su disponibilidad e integridad continuas.
A.11.2.5-Retiro de activos	Los equipos, información o software no se deberían retirar de su sitio sin autorización previa.
A.11.2.6-Seguridad de los equipos y activos fuera de las instalaciones	Se deberían aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.
A.11.2.7-Disposición segura o reutilización de equipos	Se deberían verificar todos los elementos de equipos que contengan medios de almacenamiento, para asegurar que cualquier dato sensible o software con licencia haya sido retirado o sobrescrito en forma segura antes de su disposición o reutilización.
A.11.2.8-Equipos de usuario desatendido	Los usuarios deberían asegurarse de que a los equipos desatendidos se les dé protección apropiada.
A.11.2.9-Política de escritorio y pantalla limpios	Se debería adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información.
A.12.1.1-Documentación de los procedimientos de operación	Los procedimientos de operación se deberían documentar y poner a disposición de todos los usuarios que los necesiten.
A.12.1.2-Gestión del cambio	Se deberían controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información
A.12.1.3-Gestión de la capacidad	Para asegurar el desempeño requerido del sistema se debería hacer seguimiento al uso de los recursos, hacer los ajustes, y hacer proyecciones de los requisitos sobre la capacidad futura.
A.12.1.4-Separación de los ambientes de desarrollo, pruebas y operación	Se deberían separar los ambientes de desarrollo, prueba y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.
A.12.2.1-Controles contra códigos maliciosos.	Se deberían implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.
A.12.3.1-Copias de respaldo de la información	Se deberían hacer copias de respaldo de la información, del software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada.
A.12.4.1-Registro de eventos	Se deberían elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.
A.12.4.2-Protección de la información de registro	Las instalaciones y la información de registro se deberían proteger contra alteración y acceso no autorizado.

Controles	Descripción del control
A.12.4.3-Registros del administrador y del operador	Las actividades del administrador y del operador del sistema se deberían registrar, y los registros se deberían proteger y revisar con regularidad.
A.12.4.4-Sincronización de relojes	Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deberían sincronizar con una única fuente de referencia de tiempo.
A.12.5.1-Instalación de software en sistemas operativos	Se deberían implementar procedimientos para controlar la instalación de software en sistemas operativos.
A.12.6.1-Gestión de las vulnerabilidades técnicas	Se debería obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.
A.12.6.2-Restricciones sobre la instalación de software.	Se deberían establecer e implementar las reglas para la instalación de software por parte de los usuarios
A.12.7.1-Controles de auditorías de sistemas de información.	Los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos se deberían planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.
A.13.1.1-Controles de redes	Las redes se deberían gestionar y controlar para proteger la información en sistemas y aplicaciones.
A.13.1.2-Seguridad de los servicios de red.	Se deberían identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicios de red, ya sea que los servicios se presten internamente o se contraten externamente
A.13.1.3-Separación en las redes	Los grupos de servicios de información, usuarios y sistemas de información se deberían separar en las redes.
A.13.2.1-Políticas y procedimientos de transferencia de información	Se debería contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicación
A.13.2.2-Acuerdos sobre transferencia de información	Los acuerdos deberían tener en cuenta la transferencia segura de información del negocio entre la organización y las partes externas.
A.13.2.3-Mensajes electrónicos	Se debería proteger adecuadamente la información incluida en la mensajería electrónica.
A.13.2.4-Acuerdos de confidencialidad o de no divulgación	Se deberían identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.
A.14.1.1-Análisis y especificación de requisitos de seguridad de la información	Los requisitos relacionados con seguridad de la información se deberían incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.

Controles	Descripción del control
A.14.1.2-Seguridad de servicios de las aplicaciones en redes públicas	La información involucrada en los servicios de aplicaciones que pasan sobre redes públicas se debería proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.
A.14.1.3-Protección de transacciones de servicios de aplicaciones	La información involucrada en las transacciones de los servicios de las aplicaciones se debería proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada.
A.14.2.1-Política de desarrollo seguro	Se deberían establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos que se dan dentro de la organización.
A.14.2.2-Procedimientos de control de cambios en sistemas	Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deberían controlar mediante el uso de procedimientos formales de control de cambios.
A.14.2.3-Revisión técnica de aplicaciones después de cambios en la plataforma de operaciones	Cuando se cambian las plataformas de operación, se deberían revisar las aplicaciones críticas del negocio, y ponerlas a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización.
A.14.2.4-Restricciones en los cambios a los paquetes de software	Se deberían desalentar las modificaciones a los paquetes de software, que se deben limitar a los cambios necesarios, y todos los cambios se deberían controlar estrictamente.
A.14.2.5-Principios de construcción de los sistemas seguros	Se deberían establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.
A.14.2.6-Ambiente de desarrollo seguro	Las organizaciones deberían establecer y proteger adecuadamente los ambientes de desarrollo seguros para las tareas de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.
A.14.2.7-Desarrollo contratado externamente	La organización debería supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.
A.14.2.8-Pruebas de seguridad de sistemas	Durante el desarrollo se deberían llevar a cabo pruebas de funcionalidad de la seguridad.
A.14.2.9-Prueba de aceptación de sistemas	Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deberían establecer programas de prueba para aceptación y criterios de aceptación relacionados.
A.14.3.1-Protección de datos de prueba	Los datos de ensayo se deberían seleccionar, proteger y controlar cuidadosamente.
A.15.1.1-Política de seguridad de la información para las relaciones con proveedores	Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deberían acordar con estos y se deberían documentar.
A.15.1.2-Tratamiento de la seguridad dentro de los acuerdos con proveedores	Se deberían establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización.

Controles	Descripción del control
A.15.1.3-Cadena de suministro de tecnología de información y comunicación	Los acuerdos con proveedores deberían incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación
A.15.2.1-Seguimiento y revisión de los servicios de los proveedores	Las organizaciones deberían hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.
A.15.2.2-Gestión de cambios a los servicios de los proveedores	Se deberían gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados, y la revaloración de los riesgos.
A.16.1.1-Responsabilidades y procedimientos	Se deberían establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.
A.16.1.2-Reporte de eventos de seguridad de la información	Los eventos de seguridad de la información se deberían informar a través de los canales de gestión apropiados, tan pronto como sea posible.
A.16.1.3-Reporte de debilidades de seguridad de la información	Se debería exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen e informen cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.
A.16.1.4-Evaluación de eventos de seguridad de la información y decisiones sobre ellos.	Los eventos de seguridad de la información se deberían evaluar y se debería decidir si se van a clasificar como incidentes de seguridad de la información.
A.16.1.5-Respuesta a incidentes de seguridad de la información	Se debería dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.
A.16.1.6-Aprendizaje obtenido de los incidentes de seguridad de la información	El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debería usar para reducir la posibilidad o el impacto de incidentes futuros.
A.16.1.7-Recolección de evidencia	La organización debería definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.
A.17.1.1-Planificación de la continuidad de la seguridad de la información	La organización debería determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.
A.17.1.2-Implementación de la continuidad de la seguridad de la información	La organización debería establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.
A.17.1.3-Verificación, revisión y evaluación de la continuidad de la seguridad de la información	La organización debería verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas.
A.17.2.1-Disponibilidad de instalaciones de procesamiento de información	Las instalaciones de procesamiento de información se deberían implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.

Controles	Descripción del control
A.18.1.1-Identificación de la legislación aplicable y de los requisitos contractuales	Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes, y el enfoque de la organización para cumplirlos, se deberían identificar y documentar explícitamente y mantenerlos actualizados para cada sistema de información y para la organización.
A.18.1.2-Derechos de propiedad intelectual	Se deberían implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados.
A.18.1.3-Protección de registros	Los registros se deberían proteger contra perdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.
A.18.1.4-Privacidad y protección de información de datos personales	Cuando sea aplicable, se deberían asegurar la privacidad y la protección de la información de datos personales, como se exige en la legislación y la reglamentación pertinentes.
A.18.1.5-Reglamentación de controles criptográficos	Se deberían usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes
A.18.2.1-Revisión independiente de la seguridad de la información	El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información) se deberían revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.
A.18.2.2-Cumplimiento con las políticas y normas de seguridad	Los directores deberían revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad.
A.18.2.3-Revisión del cumplimiento técnico	Los sistemas de información se deberían revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.

Tabla 21. *Lista de controles anexo A Fuente: Tomado de ISO 27001*

Acciones para dar cumplimiento al control

En **columna AA** titulada **"**Acciones para dar cumplimiento al control**"** se deben enunciar las acciones para dar cumplimiento a los controles propuestos, describiendo de forma clara y completa las actividades que se llevarán a cabo para implementar o ejecutar cada control. La redacción de estas acciones debe iniciar con un verbo en infinitivo, como, por ejemplo: realizar, socializar, divulgar, asignar o formular. Es importante que cada acción sea específica y esté directamente relacionada con el control correspondiente, proporcionando una guía concreta sobre cómo se implementará dicho control en la práctica.

Responsable de la gestión del control

En la **columna AB** titulada **"**responsable de la gestión del control**"** se debe describir el rol del responsable de la ejecución del control (dueño del riesgo), es decir que no se debe diligenciar con nombres de personas. Ej.

Líder del proceso, coordinador, enlace del proceso, funcionario, contratista, tercero, oficina, grupo de trabajo, dirección, entre otros.

Periodicidad para el cumplimiento de las acciones del control

En la **columna AC** titulada "periodicidad para el cumplimiento de las acciones del control" se debe seleccionar, de la lista proporcionada, la frecuencia con la que se realizará la revisión y se dejará evidencia de la ejecución del control. Por ejemplo, en el caso de realizar copias de seguridad, la periodicidad podría ser mensual o ajustarse según la ubicación y naturaleza de la información. Es importante documentar tanto la frecuencia elegida como las evidencias de cada ejecución del control.

Periodicidad
Diario
Semanal
Quincenal
Mensual
Bimensual
Trimestral
Cuatrimestral
Semestral
Anual
Permanente
Bajo Demanda
N/A

Tabla 22. *Frecuencia de ejecución de los controles*

Producto o evidencia de cumplimiento

En la columna AD titulada "producto o evidencia de cumplimiento" se debe diligenciar de forma clara y concisa la evidencia que debe aportar como cumplimiento de la ejecución del control.

- Análisis y evaluación de los controles – Atributos:

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

Características			Descripción	Peso
Atributos de eficiencia	Tipo	Preventivo	Va hacia las causas del riesgo, aseguran el resultado final esperado	25%
		Detectivo	Detecta que algo ocurre y devuelve el proceso a los controles preventivos. Se pueden generar reprocesos.	15%
		Correctivo	Dado que permiten reducir el impacto de la materialización del riesgo, tienen un costo en su implementación	10%
	Implementación	Automático	Son actividades de procesamiento o validación de información que se ejecutan por un sistema y/o aplicativo de manera automática sin la intervención de personas para su realización.	25%
		Manual	Controles que son ejecutados por una persona, tiene implícito el error humano.	15%
Atributos 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 evidenciar la ejecución del control.	-
		Sin registro	El control no deja registro de la ejecución del control.	-

Tabla 23. *Atributos de para el diseño del control. Fuente: DAFP.2020*

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

Controles y sus características				Peso
CONTROL 1 La profesional del área de contratos verifica que la información suministrada por el proveedor corresponda con los requisitos establecidos de contratación a través de una lista de chequeo donde están los requisitos de información y la revisión con la información física suministrada por el proveedor, los contratos que cumplen son registrados en el sistema de información de contratación.	Tipo	Preventivo	x	25%
		Detectivo		
		Correctivo		
	Implementación	Automático		
		Manual	x	15%
	Documentación	Documentado	x	
		Sin documentar		
	Frecuencia	Continua	x	
		Aleatoria		
	Evidencia	Con registro	x	
		Sin registro		
Total, Valoración Control 1			40%	

Controles y sus características				Peso
CONTROL 2 El jefe de contratos verifica en el sistema de información de contratación la información registrada por el profesional asignado y aprueba el proceso para firma del ordenador del gasto, en el sistema de información queda el registro correspondiente, en caso de encontrar inconsistencias, devuelva el proceso al profesional de contratos asignados.	**Tipo**	Preventivo		
		Detectivo	x	**15%**
		Correctivo		
	Implementación	Automático		
		Manual	x	**15%**
	Documentación	Documentado	x	
		Sin documentar		
	Frecuencia	Continua	x	
		Aleatoria		
	Evidencia	Con registro	x	
		Sin registro		
Total, Valoración Control 2			**30%**	

Diagrama 12. *Ejemplo aplicado a la tabla de atributos. Fuente: Guía para la Administración del Riesgo y el Diseño de Controles en entidades Públicas-DAFP. 2020.*

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

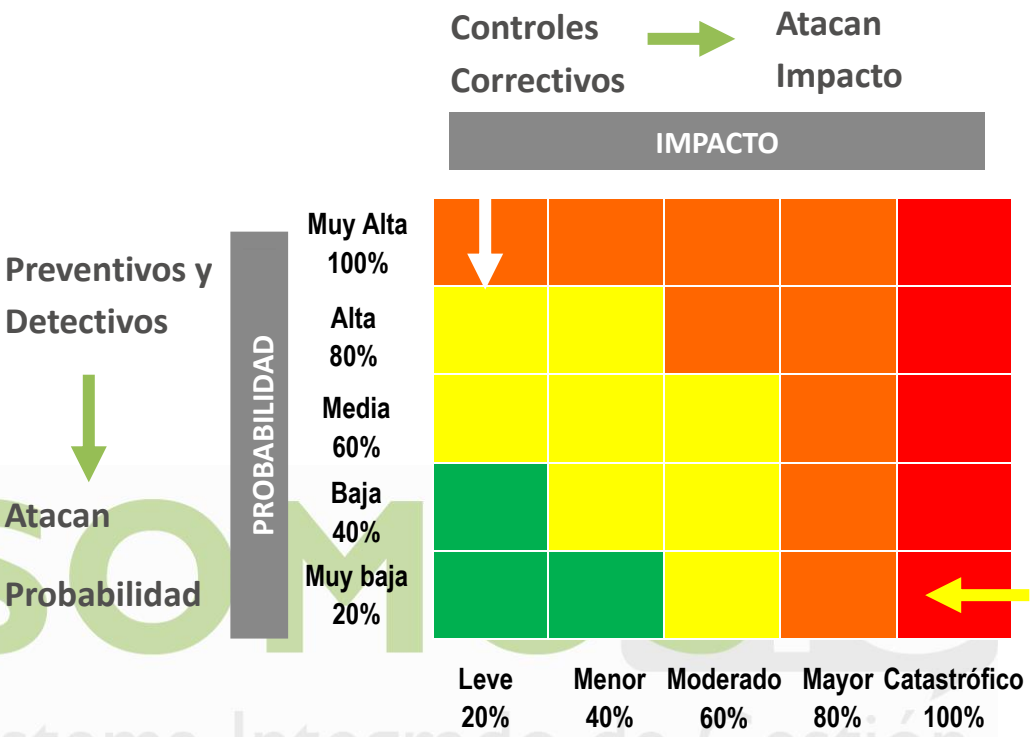


Diagrama 13. *Movimiento en la matriz de calor acorde con el tipo de control. Fuente: Guía para la Administración del Riesgo y el Diseño de Controles en entidades Públicas-DAFP. 2020.*

Para los **riesgos de corrupción** se debe tener en cuenta:

- <u>Valoración de los controles – diseño de controles</u>

Se cuenta con la siguiente clasificación de las actividades de control:

- Controles preventivos: Controles que están diseñados para evitar un evento no deseado en el momento en que se produce. Este tipo de controles intentan evitar la ocurrencia de los riesgos que puedan afectar el cumplimiento de los objetivos.

- Controles detectivos: Controles que están diseñados para identificar un evento o resultado no previsto después de que se haya producido. Buscan detectar la situación no deseada para que se corrija y se tomen las acciones correspondientes.

Al momento de definir si un control o los controles mitigan de manera adecuada el riesgo se deben considerar, desde la redacción del mismo, las siguientes variables:

- Paso 1: Debe tener definido el responsable de llevar a cabo la actividad de control. Persona asignada para ejecutar el control. Debe tener la autoridad, competencias y conocimientos para ejecutar el control dentro del proceso y sus responsabilidades deben ser adecuadamente segregadas o redistribuidas entre diferentes individuos, para reducir así el riesgo de error o de actuaciones irregulares o fraudulentas. Si ese responsable quisiera hacer algo indebido, por sí solo, no lo podría hacer. Si la respuesta es que cumple con esto, quiere decir que el control está bien diseñado, si la respuesta es que no cumple, tenemos que identificar la situación y mejorar el diseño del control con relación a la persona responsable de su ejecución.

- Paso 2: Debe tener una periodicidad definida para su ejecución. El control debe tener una periodicidad específica para su realización (diario, mensual, trimestral, anual, etc.) y su ejecución debe ser consistente y oportuna para la mitigación del riesgo. Por lo que en la periodicidad se debe evaluar si este previene o se detecta de manera oportuna el riesgo. Una vez definido el paso 1 - responsable del control, debe establecerse la periodicidad de su ejecución.
  Cada vez que se releva un control debemos preguntarnos si la periodicidad en que este se ejecuta ayuda a prevenir o detectar el riesgo de manera oportuna. Si la respuesta es SÍ, entonces la periodicidad del control está bien diseñada.

- Paso 3: Debe indicar cuál es el propósito del control. El control debe tener un propósito que indique para qué se realiza, y que ese propósito conlleve a prevenir las causas que generan el riesgo (verificar, validar, conciliar, comparar, revisar, cotejar) o detectar la materialización del riesgo, con el objetivo de llevar a cabo los ajustes y correctivos en el diseño del control o en su ejecución. El solo hecho de establecer un procedimiento o contar con una política por sí sola, no va a prevenir o detectar la materialización del riesgo o una de sus causas. Siguiendo las variables a considerar en la evaluación del diseño de control revisadas, veamos algunos ejemplos de cómo se deben redactar los controles, incluyendo el propósito del control, es decir, lo que este busca.

- Paso 4: Debe establecer el cómo se realiza la actividad de control. El control debe indicar el cómo se realiza, de tal forma que se pueda evaluar si la fuente u origen de la información que sirve para ejecutar el control, es confiable para la mitigación del riesgo. Cuando estemos evaluando el control debemos preguntarnos si la fuente de información utilizada es confiable.

- Paso 5: Debe indicar qué pasa con las observaciones o desviaciones resultantes de ejecutar el control. El control debe indicar qué pasa con las observaciones o desviaciones como resultado de ejecutar el control. Al momento de evaluar si un control está bien diseñado para mitigar el riesgo, si como resultado de un control preventivo se observan diferencias o aspectos que no se cumplen, la actividad no debería continuarse hasta que se subsane la situación o si es un control que detecta una posible materialización de un riesgo, deberían gestionarse de manera oportuna los correctivos o aclaraciones a las diferencias presentadas u observaciones.

- Paso 6: Debe dejar evidencia de la ejecución del control. El control debe dejar evidencia de su ejecución. Esta evidencia ayuda a que se pueda revisar la misma información por parte de un tercero y llegue a la misma conclusión de quien ejecutó el control y se pueda evaluar que el control realmente fue ejecutado de acuerdo con los parámetros establecidos y descritos anteriormente.

Partiendo de lo anterior, en el momento de realizar el análisis y evaluación del diseño del control se deben tener en cuenta las variables mostradas por medio de la Tabla 24. Peso o participación de cada variable en el diseño del control.

Criterio de evaluación	Opción de respuesta al criterio de evaluación	Peso en la evaluación del diseño del control
Asignación del responsable	Asignado	15
	No Asignado	0
Segregación y autoridad del responsable	Adecuado	15
	Inadecuado	0
Periodicidad	Oportuna	15
	Inoportuna	0
Propósito	Prevenir	15
	Detectar	10
	No es un control	0
Cómo se realiza la actividad de control	Confiable	15
	No confiable	0
Qué pasa con las observaciones o desviaciones	Se investigan y resuelven oportunamente	15
	No se investigan y resuelven oportunamente	0
Evidencia de la ejecución del control	Completa	10
	Incompleta	5
	No existe	0

Tabla 24. *Peso o participación de cada variable en el diseño del control. Fuente: DAFP.2018*

Una vez calificado el diseño del control se debe establecer la evaluación de acuerdo con la siguiente tabla:

Rango de calificación del diseño	Resultado – peso en la evaluación del diseño del control
Fuerte	Calificación entre 96 y 100
Moderado	Calificación entre 86 y 95
Débil	Calificación entre 0 y 85

Tabla 23. *Tabla de Evaluación del Diseño del Control. Fuente: DAFP. 2018.*

Si el resultado de las calificaciones del control, o el promedio en el diseño de los controles, está por debajo de 96%, se debe establecer un plan de acción que permita tener un control o controles bien diseñados.

Teniendo en cuenta que el solo diseño del control no es garantía de la acción de este frente a la prevención o mitigación de la materialización del riesgo se debe evaluar si el control se ejecuta de acuerdo con la siguiente calificación:

Rango de calificación de la ejecución	Resultado – peso de la ejecución del control
Fuerte	El control se ejecuta de manera consistente por parte del responsable.
Moderado	El control se ejecuta algunas veces por parte del responsable.
Débil	El control no se ejecuta por parte del responsable.

Tabla 26. *Tabla de Evaluación de la Ejecución del Control. Fuente: DAFP.2018.*

Por último, se debe realizar la calificación de la solidez del control teniendo en cuenta los resultados de la calificación del diseño del control y de la ejecución de este, la calificación de la solidez de cada control asumirá la calificación del diseño o ejecución con menor calificación entre fuerte, moderado y débil. tal como se detalla en la siguiente tabla:

Peso del diseño de cada control	Peso de la ejecución de cada control	Solidez individual de cada control: fuerte: 100 Moderado 50 Débil 0	Debe establecer acciones para fortalecer el control Sí / No
Fuerte: calificación entre 96 y 100	fuerte (siempre se ejecuta)	fuerte + fuerte = fuerte	No
	moderado (algunas veces)	fuerte + moderado = moderado	Sí
	débil (no se ejecuta)	fuerte + débil = débil	Sí
Moderado: calificación entre 86 y 95	fuerte (siempre se ejecuta)	moderado + fuerte = moderado	Sí
	moderado (algunas veces)	moderado + moderado = moderado	Sí
	débil (no se ejecuta)	moderado + débil = débil	Sí
Débil: calificación entre 0 y 85	fuerte (siempre se ejecuta)	débil + fuerte = débil	Sí
	moderado (algunas veces)	débil + moderado = débil	Sí
	débil (no se ejecuta)	débil + débil = débil	Sí

Tabla 27. *Tabla de Evaluación de la Solidez del Control. Fuente: DAFP.2018.*

7.4.3 NIVEL DE RIESGO (RIESGO RESIDUAL)

Para los **riesgos de gestión, ambientales y de seguridad de la información,** 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, esto quiere decir que una vez se aplica el valor de uno de los controles, el siguiente control se aplicará con el valor resultante luego de la aplicación del primer control.

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

Diagrama 14. *Aplicación de controles para establecer el riesgo residual. Fuente: Guía para la Administración del Riesgo y el Diseño de Controles en entidades Públicas-DAFP. 2020.*

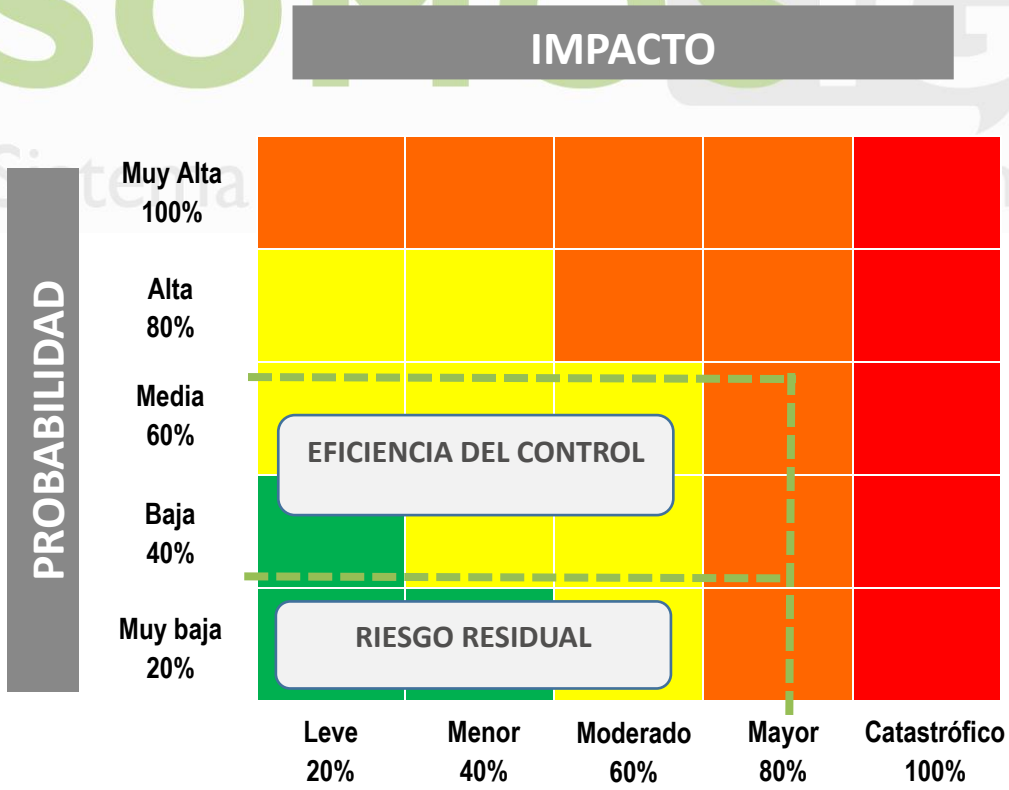


Diagrama 15. *Movimiento en la matriz de calor con el ejemplo propuesto. Fuente: Guía para la Administración del Riesgo y el Diseño de Controles en entidades Públicas-DAFP. 2020.*

Nota: En caso de no contar con controles correctivos, el impacto residual es el mismo calculado inicialmente.

Con respecto a los **riesgos de corrupción,** para determinar los riesgos residuales se debe evaluar el impacto de todos los controles diseñados por cada riesgo, por lo que hay que consolidar el conjunto de los controles asociados a las causas, para evaluar si estos de manera individual y en conjunto sí ayudan al tratamiento de los riesgos. La solidez del conjunto de controles se obtiene calculando el promedio aritmético simple de los controles por cada riesgo.

Calificación de la Solidez del Conjunto de Controles	
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.

Tabla 248. *Tabla de calificación de la solidez del conjunto de controles. Fuente: DAFP.2018.*

Una vez terminado de calificar el conjunto de controles para cada riesgo, se debe establecer el desplazamiento de un riesgo inherente en su probabilidad o impacto para el cálculo del riesgo residual lo cual se realizará de acuerdo con la siguiente tabla:

Solidez del conjunto de controles	Controles ayudan a disminuir la probabilidad	Controles ayudan a disminuir el impacto	# Columnas en la matriz de riesgo que se desplaza en el eje de probabilidad	# Columnas en la matriz de riesgo que se desplaza en el eje de 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	Directamente	1	1
Moderado	Directamente	Indirectamente	1	0
Moderado	Directamente	No disminuye	1	0
Moderado	No disminuye	Directamente	0	1

Tabla 2925. *Resultados de los posibles desplazamientos de la probabilidad y del impacto de los riesgos. Fuente: DAFP.2018.*

7.4.4 TRATAMIENTO DEL RIESGO

El tratamiento implica la selección de una o varias opciones para el manejo de los riesgos identificados, evaluados y valorados. Dentro de las opciones y luego de determinar la zona de riesgo, se pueden contemplar las siguientes:

- **Evitar el riesgo:** Cuando los escenarios de riesgo identificado se consideran demasiado extremos se puede tomar una decisión para evitar el riesgo, mediante la cancelación de una actividad o un conjunto de actividades.

- **Reducir el riesgo:** Después de realizar un análisis y considerar que el nivel de riesgo es alto se determina tratarlo mediante transferencia o mitigación del riesgo.
  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.

- **Mitigar el riesgo:** Después de realizar un análisis y considerar los niveles de riesgo se implementan acciones que mitiguen el nivel de riesgo. No necesariamente es un control adicional.
  Para mitigar/tratar los riesgos de seguridad digital se deben emplear como mínimo los controles del anexo A de la ISO/IEC 27001.

- **Transferir o compartir el riesgo:** Después de realizar un análisis, se considera que la mejor estrategia es tercerizar el proceso o trasladar el riesgo a través de seguros o pólizas.
  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.
  La responsabilidad económica recae sobre el tercero, pero no se transfiere la responsabilidad sobre el tema reputacional.
  Nota: Los riesgos de corrupción se pueden compartir, pero no se puede transferir su responsabilidad.

- **Aceptar el riesgo:** No se adopta ninguna medida que afecte la probabilidad o el impacto del riesgo. Se determina asumir el riesgo conociendo lo efectos de su posible materialización. Ningún riesgo de corrupción podrá ser aceptado.

La selección de una o más opciones de tratamiento, requiere del análisis costo-beneficio, acompañado de elementos como la viabilidad jurídica, técnica e institucional de la opción u opciones a implementar y la aprobación del dueño del proceso o la dirección según sea el caso.

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

7.5 MONITOREO Y REVISIÓN

El monitoreo y revisión tiene como propósito valorar la efectividad de los controles establecidos por la entidad, el nivel de ejecución de los planes de manejo o tratamiento de los riesgos que permiten asegurar los resultados de la gestión, así como detectar las desviaciones y tendencias para generar recomendaciones sobre el

mejoramiento de los procesos, y determinar si existen cambios en el contexto interno o externo, incluyendo los cambios en los criterios de riesgo y en el propio riesgo.

Responsables de los procesos

El monitoreo y revisión de la gestión de riesgos, está alineada con la dimensión de "Control Interno", del Modelo Integrado de Planeación y Gestión – MIPG, que se desarrolla con el MECI a través de un esquema de asignación de responsabilidades y roles, el cual se distribuye en diversos servidores de la entidad en el marco de las líneas de defensa así (Fuente: Manual MIPG)

Línea Estratégica: Define el marco general para la gestión del riesgo y el control, mediante el establecimiento de la política de administración del riesgo. Conformada por la Alta Dirección en el marco del Comité Institucional de Coordinación de Control Interno.

1era línea de defensa: La gestión operacional se encarga de desarrollar e implementar procesos de control y gestión de riesgos a través de su identificación, análisis, evaluación, control y mitigación. A cargo de los gerentes públicos y líderes de los procesos, programas y proyectos de la entidad.

Tiene como rol principal: diseñar, implementar los controles y gestionar de manera directa en el día a día los riesgos de la entidad.

Así mismo, 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.

De acuerdo con lo anterior, cada líder de proceso debe mantener la traza o documentación respectiva de todas las actividades realizadas que garanticen de forma razonable que dichos riesgos no se materializarán y por ende que los objetivos del proceso se cumplan.

2da 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. Ocupados por cargos del nivel directivo o asesor (media o alta gerencia), quienes realizan labores de supervisión sobre temas transversales para la entidad y rinden cuentas ante la Alta Dirección.

A cargo de los servidores que tienen responsabilidades directas en el monitoreo y evaluación de los controles y la gestión del riesgo: Jefes de planeación, supervisores e interventores de contratos o proyectos, coordinadores de sistemas de gestión de la Entidad, líderes o coordinadores de contratación, financiera y de TIC, entre otros.

El rol principal es monitorear la gestión de riesgo y control ejecutada por la primera línea de defensa, complementando su trabajo, así como, el aseguramiento sobre el diseño apropiado de los controles, de manera que pueda orientar y generar alertas a las personas que hacen parte de la 1ª línea de defensa, así como a la Alta Dirección (Línea Estratégica)

3ra línea de defensa: A cargo de la Oficina de Control Interno, auditoría interna o quien haga sus veces. El rol principal es proporcionar un aseguramiento basado en el más alto nivel de independencia y objetividad sobre la efectividad del Sistema de Control Interno.

El alcance de este aseguramiento se realiza a través de la auditoría interna que cubre todos los componentes del Sistema de Control Interno. Evalúan de manera independiente y objetiva los controles de 2ª línea de defensa para asegurar su efectividad y cobertura; así mismo, evalúa los controles de 1ª línea de defensa que no se encuentren cubiertos o inadecuadamente cubiertos por la 2ª línea de defensa.

Las interacciones entre la 2ª línea de defensa (proveedores internos de aseguramiento) y la 3ª línea de defensa y estas con los proveedores externos de aseguramiento (organismos de control y otras instancias de supervisión o vigilancia) son representadas en el mapa de aseguramiento, herramienta que permite coordinar las diferentes actividades de aseguramiento, visualizar el esfuerzo en común y mitigar los riesgos de una manera mucho más integral.

Adicionalmente, tiene como roles el liderazgo estratégico, enfoque hacia la prevención, evaluación de la gestión del riesgo, relación con entes externos de control y el de evaluación y seguimiento.

Línea	Responsable	Responsabilidades
Línea Estratégica	Alta Dirección	● Analizar los riesgos y amenazas institucionales frente al cumplimiento de los planes estratégicos (objetivos, metas, indicadores).
	Comité Institucional de Coordinación de Control Interno	● Definir el marco general, roles y responsabilidades para la gestión del riesgo (política de administración del riesgo) y el control de riesgos. ● Identificar cambios en el contexto estratégico que puedan generar modificaciones a los riesgos existentes o nuevos riesgos. ● Revisar que los riesgos identificados tengan el impacto en el cumplimiento de objetivos estratégicos, estén alineados con la misión y la visión institucional, así como, su desdoble hacia los objetivos de los procesos. ● Revisar y tomar decisiones frente a los Planes de contingencia formulados para cada uno de los riesgos materializados con el fin de evitar su repetición. ● Realizar el análisis de eventos y riesgos críticos que tienen un nivel de severidad muy alto frente a los cuales se deben tomar decisiones. ● Hacer seguimiento a los resultados de las evaluaciones realizadas por Control Interno o Auditoría Interna frente a la administración de riesgos. ● Analizar los cambios en el entorno interno y externo que puedan tener un impacto significativo en la entidad y que puedan generar cambios en la estructura de riesgos y controles. ● Revisar los informes presentados de los eventos de riesgos que se han materializado en la entidad, incluyendo los riesgos de corrupción, así como las causas que dieron origen a esos eventos.

Línea	Responsable	Responsabilidades
		● Hacer seguimiento y pronunciarse sobre el perfil de riesgo inherente y residual de la entidad, incluyendo los riesgos de corrupción y de acuerdo con las políticas de tolerancia, establecidas y aprobadas.
	Comité Institucional de Gestión y Desempeño	● Aprobar el mapa de riesgos actualizado para cada vigencia. ● Tomar decisiones frente a los resultados de la gestión del riesgo, monitoreo y seguimiento del mapa de riesgos institucional. ● Revisar el cumplimiento a los objetivos institucionales y de procesos y sus indicadores e identificar en caso de que no se estén cumpliendo, los posibles riesgos que se están materializando.
1ª Línea de defensa	Jefes de área o líderes de proceso, facilitadores y sus equipos de trabajo.	● Implementar la G-E-SIG-05 "Guía de Administración del Riesgo". ● Implementar y mantener los controles establecidos en el mapa y plan de manejo de riesgos. ● Implementar acciones correctivas en los casos que se detecten deficiencias del control. ● Formular e implementar los planes de contingencia en caso de materialización de los riesgos. ● Revisar los cambios en el contexto estratégico que puedan generar modificaciones a los riesgos existentes o nuevos riesgos de los procesos y actualizar la matriz F-E-SIG-28 mapa de riesgos institucional. ● Revisión del adecuado diseño y ejecución de los controles establecidos para la mitigación de los riesgos. ● Revisar que las actividades de control de sus procesos se encuentren documentadas y actualizadas en los procedimientos. ● Revisar el cumplimiento de los objetivos de sus procesos y sus indicadores e identificar en caso de que no se estén cumpliendo, los posibles riesgos que se están materializando en el cumplimiento de los objetivos. ● Revisar y reportar a la Oficina Asesora de Planeación, los riesgos que se han materializado, así como, las causas que dieron origen a esos eventos, para hacer seguimiento al plan de contingencia formulado. ● Revisar los Planes de contingencia formulados para cada uno de los riesgos materializados con el fin de tomar medidas para evitar su repetición y lograr el cumplimiento a los objetivos. ● Revisar y hacer seguimiento al cumplimiento de las actividades y planes de manejo aprobados, con relación a la gestión de riesgos. ● Reportar oportunamente el avance de las acciones del plan de manejo e implementación de controles del mapa de riesgos del proceso de los cuales es responsable.
2ª Línea de defensa	Responsables del monitoreo y evaluación de controles y gestión del riesgo: jefe de la Oficina Asesora de Planeación a través del grupo de Gestión y Desempeño Institucional - GDI, coordinadores de equipos de trabajo, supervisores de contratos, Comité de contratación, áreas	● Asegura que los controles y procesos de gestión del riesgo de la 1ª Línea de defensa sean apropiados y funcionen correctamente y determina las recomendaciones para el fortalecimiento de estos. ● Ejerce el control y la gestión de riesgos, las funciones de cumplimiento, seguridad y calidad. ● Supervisa la implementación de prácticas de gestión de riesgo eficaces por parte de la primera línea y ayuda a los responsables de riesgos a distribuir información adecuada sobre riesgos a todos los servidores del Ministerio.

Línea	Responsable	Responsabilidades
	financieras y responsables de sistemas de gestión.	● Revisar los cambios en el contexto estratégico que puedan generar modificaciones a los riesgos existentes o nuevos riesgos de los procesos con el fin de solicitar y apoyar en la actualización de la matriz F-E-SIG-28 mapa de riesgos institucional. ● Revisar que los riesgos identificados tengan el impacto en el cumplimiento de objetivos estratégicos, estén alineados con la misión y la visión institucional, así como, su desdoble hacia los objetivos de los procesos y realizar las recomendaciones a que haya lugar. ● Revisar el perfil de riesgo inherente y residual por cada proceso y consolidado y pronunciarse sobre cualquier riesgo que este por fuera del perfil de riesgo de la entidad. ● Hacer seguimiento a que las actividades de control establecidas para la mitigación de los riesgos de los procesos se encuentren documentadas y actualizadas en los procedimientos. ● Revisar los Planes de contingencia formulados para cada uno de los riesgos materializados con el fin de tomar medidas para evitar su repetición y lograr el cumplimiento a los objetivos.
3ª Línea de defensa	Oficina de Control Interno	● Proporcionar información sobre la efectividad del Sistema de Control Interno, la operación de la primera y segunda línea de defensa con un enfoque basado en riesgos. ● La función de auditoría interna, a través de un enfoque basado en el riesgo, proporciona aseguramiento sobre la eficacia institucional, gestión de riesgos y control interno a la Alta Dirección, incluyendo el funcionamiento de la primera y segunda línea de defensa. ● Revisar los cambios en el contexto estratégico que puedan generar modificaciones a los riesgos existentes o nuevos riesgos de los procesos, con el fin de que se identifique y actualice la matriz F-E-SIG-28 mapa de riesgos institucional por parte de los responsables. ● Revisar que los riesgos identificados tengan el impacto en el cumplimiento de objetivos estratégicos, estén alineados con la misión y la visión institucional, así como, su desdoble hacia los objetivos de los procesos y realizar las recomendaciones a que haya lugar. ● Revisar que se hayan identificado los riesgos significativos que afectan en el cumplimiento de los objetivos de los procesos, además de incluir los riesgos de corrupción. ● Revisar el adecuado diseño y ejecución de los controles para la mitigación de los riesgos que se han establecido por parte de la primera línea de defensa y realizar las recomendaciones y seguimiento para el fortalecimiento de estos. ● Revisar el perfil de riesgo inherente y residual por cada proceso consolidado y pronunciarse sobre cualquier riesgo que este por fuera del perfil de riesgo de la entidad o que su calificación del impacto o probabilidad del riesgo no es coherente con los resultados de las auditorías realizadas. ● Para mitigar los riesgos de los procesos revisar que se encuentren documentados y actualizados los procedimientos y los planes de mejoramiento resultado de las auditorías efectuadas; que se lleven a cabo de manera oportuna, se establezcan las causas raíz del problema y se evite, en lo posible, la repetición de hallazgos y la materialización de los riesgos.

Tabla 30. *Responsabilidad frente a la gestión del riesgo Adaptada Fuente: DAFP. 2018*

La Oficina de Tecnologías de la Información y la Comunicación – OTIC liderará el proceso de formulación de los riesgos de seguridad de la información del Ministerio, formulación que una vez aprobada por los líderes de proceso y el Comité Institucional de Gestión y Desempeño, será consolidada en el mapa de riesgos institucional por parte de la Oficina Asesora de Planeación. Este ejercicio se articulará con el cronograma de actualización de los riesgos de gestión y corrupción para cada vigencia, liderado por la Oficina Asesora de Planeación.

La Oficina Asesora de Planeación realizará el monitoreo únicamente frente al cumplimiento del reporte por parte de los líderes de cada proceso y entrega de las evidencias del avance de las acciones y controles de los riesgos de seguridad de la información del Ministerio.

Corresponde a la Oficina de Tecnologías de la Información y la Comunicación – OTIC, realizar el acompañamiento técnico a las dependencias para que ellas puedan atender las observaciones, hallazgos o recomendaciones que realice la Oficina de Control Interno, entes reguladores o cualquier otra instancia, frente a los riesgos de seguridad de la información del Ministerio y la efectividad de los controles implementados, como líder del Modelo de Seguridad y Privacidad de la Información – MSPI.

Los riesgos se actualizan y validan de manera permanente y en cualquier momento de ser necesario, considerando las condiciones de operación internas o externas. Cada líder de proceso actualiza el análisis de contexto, riesgos y controles como resultado de los ejercicios de autocontrol, autoevaluación, evaluación independiente o por decisión del Comité Institucional de Coordinación de Control Interno, según estime conveniente para asegurar el cumplimiento de los objetivos del proceso.

En todo caso la revisión y actualización se realizará mínimo una vez al año con el acompañamiento de la Oficina Asesora de Planeación, la Oficina TIC según el tipo de riesgo y la asesoría de la Oficina de Control Interno.

La fecha programada para el cumplimiento de las acciones del mapa de riesgos aprobado, será hasta el primer trimestre de la siguiente vigencia, con el fin realizar el seguimiento y monitoreo del cierre de la gestión.

De otra parte y en concordancia con “La Guía para la Gestión del riesgo de Corrupción” de la Presidencia de la República, los riesgos de corrupción actualizados se publican a más tardar el 31 de enero de cada año, se realizarán seguimientos periódicos sobre los posibles actos de corrupción mediante la evaluación de los riesgos de corrupción, equiparando dicho seguimiento a las fechas establecidas de seguimiento al Plan Anticorrupción y atención al ciudadano ahora Programa de Transparencia y Ética Pública, las cuales son 3 veces al año empezando el 1ero con corte al 30 de abril, el 2do con corte al 31 de agosto y el 3ero con corte al 31 de diciembre.

Dicho seguimiento se publicará en la página web de la entidad o en lugar de fácil acceso al ciudadano.

Se puede considerar la eliminación de los riesgos que se encuentren en nivel de aceptación Bajo o aceptable, los cuales deberán soportar la evidencia de la implementación de sus controles existentes de manera que justifiquen la no materialización durante la vigencia.

El responsable de cada proceso registra dos veces en el año en el mapa de riesgos o de acuerdo con las solicitudes de monitoreo de la Oficina Asesora de Planeación, el estado de la gestión de las acciones y controles formulados junto con las evidencias correspondientes, describiendo concretamente si hubo o no riesgos materializados, así mismo, se deberá analizar el cumplimiento de los indicadores de gestión y su relación con la materialización de los riesgos.

Si se identifican riesgos materializados por cualquiera de las líneas de defensa, de manera inmediata se ejecutan las acciones de contingencia para su tratamiento.

RIESGOS MATERIALIZADOS

Cuando se detecte la materialización de los riesgos, se activará el plan de contingencia del riesgo y se realizarán las siguientes acciones:

a) Materialización de riesgos detectada por parte del líder del proceso (primera línea de defensa):

- Si el riesgo es de corrupción se deberá informar a la Oficina Asesora de Planeación como representante del Ministro para el Sistema Integrado de Gestión (Resolución 2140 de 2017), sobre el hecho encontrado. De considerarlo necesario, realizar la denuncia ante el ente de control respectivo.
- Si el riesgo es de gestión, se deberá realizar el análisis de causas y determinar acciones, análisis y actualización del mapa de riesgos.

b) Materialización de riesgos detectada por la segunda línea de defensa:

- En los casos de riesgos de corrupción detectado por la segunda Línea de defensa, se debe:
  - Informar sobre el hecho encontrado a la Oficina de Control Interno, para lo de su competencia
  - Informar al líder del proceso, para revisar el mapa de riesgos y sus controles asociados, verificar que se tomaron las acciones y que se actualizó el mapa de riesgos.
- En los casos de riesgos de Gestión detectado por la segunda Línea de defensa, se debe comunicar a la Oficina de Control Interno, para lo de su competencia y al líder del proceso sobre el hecho encontrado, para que realice la revisión, análisis y acciones correspondientes para resolver el hecho y verificar que se tomaron las acciones, que se actualizó el mapa de riesgos correspondiente e informar a la Alta Dirección sobre el hallazgo y las acciones tomadas.

c) Materialización de riesgos detectada por parte de la Oficina de Control Interno (tercera línea de defensa):

- Si el riesgo es de corrupción, se deberá convocar al Comité de Coordinación de Control Interno e informar sobre los hechos detectados, desde donde se tomarán las decisiones para iniciar la investigación de los hechos. Dependiendo del alcance (normatividad asociada al hecho de corrupción materializado), realizar la denuncia ante el ente de control respectivo. Facilitar el inicio de las acciones correspondientes con el líder del proceso, para revisar el mapa de riesgos y sus controles asociados. Verificar si se tomaron las acciones y si se actualizó el mapa de riesgos.
- Si el riesgo es de gestión, informar al líder del proceso sobre el hecho encontrado y orientarlo frente a la revisión, análisis y acciones correspondientes para resolver el hecho. Convocar al Comité de Coordinación de Control Interno e informar sobre la actualización realizada.

7.6 MAPA DE RIESGOS INSTITUCIONAL

El mapa de riesgos institucional, se consolida en el documento soporte DS-E-SIG-25_mapa de riesgos institucional, el cual se puede consultar en la página WEB del Ministerio en el link https://www.minambiente.gov.co/planeacion-y-seguimiento/administracion-del-riesgo/ ,así como, en el aplicativo del Sistema Integrado de Gestión **SOMOSIG** (antes denominado MADSIGestion), una vez sea aprobado por los responsables de los procesos en el Comité Institucional de Gestión y Desempeño.

Se realiza el diligenciamiento del formato F-E-SIG-28 “Mapa de riesgos institucional” que contiene el registro de los riesgos identificados, establece la clase de riesgo, identifica las causas, así como, la probabilidad e impacto, evaluando el riesgo inherente.

Posteriormente, se realiza el análisis de las estrategias que contrarresten las causas raíz, incluyendo las actividades de control, valorando los controles para determinar el riesgo residual y establecer la opción de tratamiento a la que corresponden.

Mediante la definición del plan de manejo del riesgo se relaciona el soporte o indicador con el que se evidenciará el cumplimiento de cada actividad, el responsable de adelantarla (relacionando el cargo) y el tiempo específico para su cumplimiento.

Al final de todas las actividades de control establecidas en el plan de manejo del riesgo para atacar las causas del mismo, se debe relacionar el plan de contingencia a implementar una vez el riesgo se materialice, teniendo en cuenta que este tipo de acciones son de aplicación inmediata y a corto plazo para restablecer, cuanto antes, la normalidad de las actividades para el logro de los objetivos del proceso.

Por último, se evidencia el monitoreo y seguimiento frente a las responsabilidades de la 1era, 2da y 3era línea de defensa en el marco del proceso de administración del riesgo

8 COMUNICACIÓN Y CONSULTA

La comunicación y la consulta deberán surtirse en todas las etapas de construcción del mapa de riesgos institucional en el marco de un proceso participativo que involucre actores internos y externos del ministerio.

Esta etapa tiene como principales objetivos los siguientes:

1. Ayudar a establecer el contexto estratégico
2. Ayudar a determinar que los riesgos estén correctamente identificados.
3. Reunir diferentes áreas de experticias para el análisis de los riesgos.
4. Fomentar la gestión de riesgos.

Una vez surtido este proceso de consulta es de suma importancia que se comunique internamente el mapa de riesgos institucional y externamente el mapa de riesgos de corrupción. De tal manera que funcionarios y contratistas del ministerio; así como las partes interesadas, conozcan la forma como se estructuran los riesgos de gestión y corrupción.