POLÍTICA DE ADMINISTRACIÓN DE RIESGOS

Aprobada en Comité Institucional de Coordinación de Control Interno en julio 27/2022

ESO RIONEGRO S.A.S

Empresa de Seguridad del Oriente S.A.S.
www.eso.gov.co
Cra. 46 # 30 - 425
Vereda El Rosal
Rionegro, Antioquia
57 (4) 520 40 60 ext. 1900
NIT 900.984.614-9

CONTENIDO

POLÍTICA DE ADMINISTRACIÓN DE RIESGOS

De conformidad con la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, versión 5 de diciembre de 2020 y demás normas vigentes, la EMPRESA DE SEGURIDAD DE ORIENTE S.A.S. -ESO RIONEGRO S.A.S.- del orden Municipal, formula y adopta la Política de Administración de Riesgos, mediante la cual establece los lineamientos y la metodología aplicable para identificar, analizar, valorar, monitorear, administrar y tratar los riesgos que pudieran afectar positiva o negativamente el logro de los objetivos estratégicos.

1. OBJETIVO

El objetivo principal de esta Política es gestionar la identificación, análisis, valoración, tratamiento, monitoreo y seguimiento a los riesgos de Ejecución y Administración de Procesos, Fraude Externo, Daños a Activos Fijos/ Eventos Externos, Fraude Interno, Fallas Tecnológicas, Relaciones Laborales, Usuarios, Productos y Prácticas, con el fin de mitigar o eliminar efectos negativos en el logro de los Objetivos Estratégicos y de los procesos de la Empresa de Seguridad del Oriente S.A.S – ESO Rionegro S.A.S.

Tener presente que el riesgo en su tendencia más común es valorado como una amenaza, en este sentido, los esfuerzos institucionales se dirigen a reducirlo, evitarlo, transferirlo o mitigarlo; sin embargo, el riesgo puede ser analizado como una oportunidad, lo cual implica que su administración sea dirigida a maximizar los resultados que este genera.

2. ALCANCE

El manejo de los Riesgos de la entidad tendrá carácter prioritario y estratégico, fundamentado en el Modelo de Operación por Procesos. En virtud de esto, la identificación, análisis, valoración y monitoreo de los riesgos corresponderá a cada proceso de acuerdo con los objetivos estratégicos de los mismos. El requerimiento de la formulación del Mapa de Riesgos en cada vigencia cobijará a todos los procesos, entendiéndose el carácter obligatorio de su presentación en referencia a la gestión administrativa.

La Política de Riesgos aplica a todos los procesos, procedimientos, proyectos y todas las acciones y actividades ejecutadas por los servidores en el ejercicio de sus funciones. Está bajo la responsabilidad de los líderes de proceso, las tres líneas de defensa y de la Línea Estratégica de Defensa

3. TÉRMINOS Y DEFINICIONES

Riesgo: Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales. Nota: Los eventos	**Riesgo de Seguridad de la Información:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar	**Riesgo de Corrupción:** Posibilidad de que, por acción u omisión, se use el	**Probabilidad:** se entiende la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del

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.	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).	poder para desviar la gestión de lo público hacia un beneficio privado	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.
Causa: todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo	**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.	**Impacto:** las consecuencias que puede ocasionar a la organización la materialización del riesgo.	**Riesgo Inherente**: Nivel de riesgo propio de la actividad. El resultado de combinar la probabilidad con el impacto, nos permite determinar el nivel del riesgo inherente, dentro de unas escalas de severidad
Riesgo Residual: El resultado de aplicar la efectividad de los controles al riesgo inherente.	**Control:** Medida que permite reducir o mitigar un riesgo.	**Causa Inmediata:** Circunstancias bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo.	**Causa Raíz:** Causa principal o básica, corresponde a las razones por la cuales se puede presentar el riesgo.
Factores de Riesgo: Son las fuentes generadoras de riesgos.	**Confidencialidad:** Propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados	**Integridad:** Propiedad de exactitud y completitud.	**Disponibilidad:** Propiedad de ser accesible y utilizable a demanda por una entidad.
Vulnerabilidad: Representan la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.	**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	**Nivel de riesgo:** Es el valor que se determina a partir de combinar la probabilidad de ocurrencia de un evento potencialmente dañino y la magnitud del impacto que este evento traería sobre la capacidad institucional de alcanzar los objetivos. En general la fórmula del Nivel del	**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

	funcionar en el entorno digital.	Riesgo poder ser Probabilidad * Impacto, sin embargo, pueden relacionarse las variables a través de otras maneras diferentes a la multiplicación, por ejemplo, mediante una matriz de Probabilidad – Impacto.	entidad debe o desea gestionar.
Tolerancia del riesgo: Es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del Apetito de riesgo determinado por la entidad.	**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.	**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.	**Plan Anticorrupción y de Atención al Ciudadano:** Plan que contempla la estrategia de lucha contra la corrupción que debe ser implementada por todas las entidades del orden nacional, departamental y municipal.

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

4. CLASIFICACIÓN DEL RIESGO

- Permite agrupar los riesgos identificados, se clasifica cada uno de los riesgos en las siguientes categorías:
- Ejecución y administración de procesos
- Pérdidas derivadas de errores en la ejecución y administración de procesos.
- Fraude externo
- Pérdida derivada de actos de fraude por personas ajenas a la organización (no participa personal de la entidad).
- 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.
- Fraude interno
- Pérdida debido a actos de fraude, actuaciones irregulares, comisión de hechos delictivos abuso de confianza, apropiación indebida, incumplimiento de regulaciones legales o internas de la entidad en las cuales está involucrado por lo menos 1 participante interno de la organización, son realizadas de forma intencional y/o con ánimo de lucro para sí mismo o para terceros.
- Fallas tecnológicas
- Errores en hardware, software, telecomunicaciones, interrupción de servicios básicos.
- Relaciones laborales
- Pérdidas que surgen de acciones contrarias a las leyes o acuerdos de empleo, salud o seguridad, del pago de demandas por daños personales o de discriminación.

- Usuarios, productos y prácticas
- Fallas negligentes o involuntarias de las obligaciones frente a los usuarios y que impiden satisfacer una obligación profesional frente a estos.

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

5. IDENTIFICACIÓN DEL RIESGO

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

Se aplican las siguientes fases contenidas en la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, versión 5 de diciembre de 2020.

5.1 Análisis de objetivos estratégicos y de los procesos

Este paso es muy importante, dado que todos los riesgos que se identifiquen deben tener impacto en el cumplimiento del objetivo estratégico o del proceso.

La entidad debe analizar los objetivos estratégicos y revisar que se encuentren alineados con la misión y la visión institucionales, así como su desdoble hacia los objetivos de los procesos. Se plantea la necesidad de analizar su adecuada formulación, es decir, que contengan unos atributos mínimos.

5.2 Identificación de los puntos de riesgo

Son actividades dentro del flujo del proceso donde existe evidencia o se tienen indicios de que pueden ocurrir eventos de riesgo operativo y deben mantenerse bajo control para asegurar que el proceso cumpla con su objetivo.

5.3 Identificación de áreas de impacto

El área de impacto es la consecuencia económica o reputacional a la cual se ve expuesta la organización en caso de materializarse un riesgo. Los impactos que aplican son afectación económica (o presupuestal) y reputacional. Son las fuentes generadoras de riesgos y los factores de riesgo que puede tener una entidad.

6. RESPONSABILIDADES Y COMPROMISOS FRENTE AL RIESGO

MECI está acompañado de un esquema de asignación de responsabilidades y roles para la gestión del riesgo y el control, el cual se distribuye en diversos servidores de la entidad, no siendo ésta una tarea exclusiva de las oficinas de control interno.[1]

Línea estratégica de defensa: está conformada por la Alta Dirección y el Comité Institucional de Coordinación de Control Interno. La responsabilidad de esta línea de defensa se centra en la emisión, revisión, validación y supervisión del cumplimiento de políticas en materia de control interno, gestión del riesgo, seguimientos a la gestión y auditoría interna para toda la entidad. [2]

Los aspectos clave para el Sistema de Control Interno (SCI) a tener en cuenta por parte de la **Línea Estratégica** son:[3] Definición y evaluación de la Política de Administración del Riesgo. La evaluación debe considerar su aplicación en la entidad, cambios en el entorno que puedan definir ajustes, dificultades para su desarrollo, riesgos emergentes.[4]

Primera Línea de Defensa: Esta línea se encarga del mantenimiento efectivo de controles internos, por consiguiente, identifica, evalúa, controla y mitiga los riesgos.

Los aspectos clave para el Sistema de Control Interno (SCI) a tener en cuenta por parte de la 1ª Línea:[5]

La identificación de riesgos y el establecimiento de controles, así como su seguimiento, acorde con el diseño de dichos controles, evitando la materialización de los riesgos.[6]

Segunda Línea de Defensa: esta línea de defensa está conformada por servidores que ocupan 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. Aquí se incluyen a los jefes de planeación, o quienes hagan sus veces; coordinadores de equipos de trabajo, coordinadores de sistemas de gestión, gerentes de riesgos (donde existan), líderes o coordinadores de contratación, financiera y de TIC, entre otros que se deberán definir acorde con la complejidad y misionalidad de cada organización. Esto le permite a la entidad hacer un seguimiento o autoevaluación permanente de la gestión, 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). Esta línea se asegura de que los controles y procesos de gestión del riesgo de la 1ª línea de defensa sean apropiados y funcionen correctamente, además, se encarga de supervisar la eficacia e implementación de las prácticas de gestión de riesgo, ejercicio que implicará la implementación de actividades de control específicas que permitan adelantar estos procesos de seguimiento y verificación con un enfoque basado en riesgos.[7]

---

[1] https://www.funcionpublica.gov.co/documents/28587410/34112007/Manual+Operativo+MIPG.pdf/ce5461b4-97b7-be3b-b243-781bbd1575f3?t=1638367931337
[2] Ídem al anterior
[3] Ídem al anterior
[4] Ídem al anterior
[5] Ídem al anterior
[6] Ídem al anterior
[7] Ídem al anterior

Los aspectos clave para el Sistema de Control Interno (SCI) a tener en cuenta por parte de la 2ª Línea son:[8]

• Aseguramiento de que los controles y procesos de gestión del riesgo de la 1ª Línea de Defensa sean apropiados y funcionen correctamente, supervisan la implementación de prácticas de gestión de riesgo eficaces.[9]

• Consolidación y análisis de información sobre temas claves para la entidad, base para la toma de decisiones y de las acciones preventivas necesarias para evitar materializaciones de riesgos.[10]

• Asesoría a la 1ª línea de defensa en temas clave para el Sistema de Control Interno: i) riesgos y controles[11]

Tercera Línea de Defensa: esta línea de defensa está conformada por la Oficina de Control Interno, quienes 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 y los que inadecuadamente son cubiertos por la 2ª línea de defensa.[12]

Los aspectos clave para el Sistema de Control Interno (SCI) a tener en cuenta por parte de la 3ª Línea:[13]

• A través de su rol de asesoría, orientación técnica y recomendaciones frente a la administración del riesgo en coordinación con la Oficina Asesora de Planeación o quien haga sus veces se garantiza el cumplimento efectivo de los objetivos.[14]

• Monitoreo a la exposición de la organización al riesgo y realizar recomendaciones con alcance preventivo.[15]
• Asesoría proactiva y estratégica a la Alta Dirección y los líderes de proceso, en materia de control interno y sobre las responsabilidades en materia de riesgos.[16]

• Formar a la alta dirección y a todos los niveles de la entidad sobre las responsabilidades en materia de riesgos.[17]

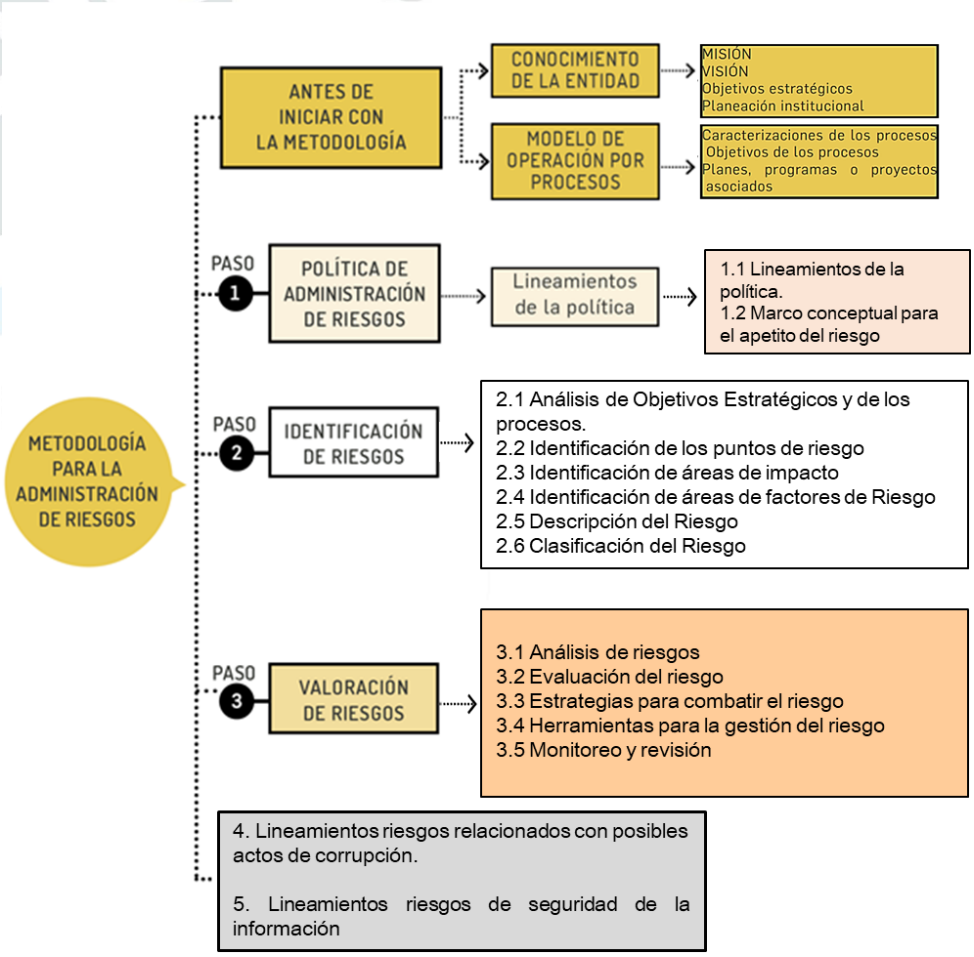
7. METODOLOGÍA PARA LA ADMINISTRACIÓN DEL RIESGO

La metodología para la administración del riesgo requiere de un análisis inicial relacionado con el estado actual de la estructura de riesgos y su gestión en la entidad, además del conocimiento de esta desde un punto de vista estratégico de la aplicación de los tres (3) pasos básicos para su desarrollo y, finalmente, de la definición e implantación de estrategias de comunicación transversales a toda la entidad para que su

[8] Ídem al anterior
[9] Ídem al anterior
[10] Ídem al anterior
[11] Ídem al anterior
[12] Ídem al anterior
[13] Ídem al anterior
[14] Ídem al anterior
[15] Ídem al anterior
[16] Ídem al anterior

efectividad pueda ser evidenciada. A continuación, se puede observar la estructura completa con sus desarrollos básicos:

Metodología para la administración del riesgo



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

7.1 CONTEXTO ESTRATÉGICO

En cada vigencia se analizará el entorno estratégico de la Empresa a partir de los siguientes factores externos (amenazas y oportunidades), internos (fortalezas y debilidades) y de procesos para el adecuado análisis de las causas del riesgo y la gestión del mismo:

7.1.1 MATRIZ DOFA

En el análisis de la matriz DOFA se hizo identificaron las siguientes Fortalezas, Debilidades, Oportunidades y Amenazas.

FORTALEZAS (Internas)
1. Buen nivel de relacionamiento con entes públicos y privados. 2. Good Will (reputación). 3. Innovación tecnológica y empresarial. 4. Régimen de contratación. 5. Aprendizaje en trámites de financiación con bancos, Findeter. 6. Experticia técnica, jurídica y financiera en proyectos. 7. Contamos con aliados estratégicos. 8. Recurso Humano calificado. 9. Contar con equipos, herramientas y parque automotor especializados

DEBILIDADES (Internas)
1. Limitado objeto social 2. Falta de capital de trabajo. 3. No existe área de desarrollo e innovación. 4. No estar certificados. 5. No contar con buen procedimiento de gestión del conocimiento 6. Alta rotación de personal. 7. Desconocimiento de procesos y procedimientos 8. Deficientes indicadores financieros

OPORTUNIDADES (Externas)
1. Ubicación geográfica estratégica. 2. Alto Desarrollo regional. 3. Alianzas estratégicas: universidades, gobernación, SENA, Fonsecon, FINDETER, IDEA, Bancos, Ministerios. 4. Participar en licitaciones públicas (SECOP). 5. Visibilizar ventaja contratación directa para soluciones rápidas 6. Integrador Tecnológico para Rionegro y otros municipios. 7. Centro de inteligencia y monitoreo regional (Gobernación Antioquia). 8. Potencialidad de clientes privados

9. Comercializar productos y servicios exitosos en el municipio de Rionegro

AMENAZAS (Externas)
1. Cambios de gobierno local. 2. Rionegro quite la desconcentración del alumbrado. 3. Injerencia en gestión de recursos humanos estratégicos. 4. Nuevos competidores IDEA, nuevas empresas municipales. 5. Incumplimientos de los pagos por parte de los clientes. 6. Inestabilidad jurídica, cambio de normatividad. 7. Exigencia de requisitos financieros que no cumple la ESO

El análisis interno específico de la Entidad da cuenta de los siguientes aspectos en los factores que se enuncian:

Financieros:

- Falta de capital de trabajo, proyectos no garantizan oportuno flujo de caja
- Deficientes indicadores financieros que impiden participar en algunos procesos
- Alta dependencia de negocios con el municipio de Rionegro
- Alta dependencia del negocio de alumbrado público.
- Incumplimientos de los pagos por parte del municipio de Rionegro
- Deficiencias en la estructuración de proyectos
- Necesidad de capitalización
- Falta de oportunidad en la liquidación de contratos

Personal:

- No contar con buen procedimiento de gestión del conocimiento
- Alta rotación de personal: desmotivación, falta de compromiso, afectación del clima laboral
- Injerencia externa en gestión de recursos humanos estratégicos.

Procesos:

- Desvíos entre los procesos establecidos y lo que se ejecuta.
- Desconocimiento de los procesos y procedimientos por parte de los servidores.
- Deficiente autogestión y auto seguimiento en algunos procesos

Tecnología:

- Desconocimiento y baja aplicabilidad de las herramientas informáticas.

- Posibles fallas en equipos de cómputo y deficiente conectividad de la red (Internet)
- No existe área de desarrollo e innovación
- Deficiencias en seguridad de información e informática
- No disponer de un plan tecnológico que garantice la continuidad del negocio

Estratégicos:

- Deficiencia en la ejecución y seguimiento estratégico
- Estructura organizacional no acorde con el crecimiento y negocios de la empresa
- Cambios de gobierno local.
- Rionegro quite la desconcentración del alumbrado
- Injerencia en gestión de recursos humanos estratégicos.
- Nuevos competidores IDEA, nuevas empresas municipales
- Inestabilidad jurídica, cambio de normatividad.
- Exigencia de requisitos financieros que no cumple la ESO
- Limitado objeto social.

Comunicación Interna:

- Poca efectividad en los canales internos (correo electrónico institucional).
- Deficiente motivación y sensibilización de los servidores para el manejo de la información.
- Desactualización de la información en la página WEB y falta de priorizar los contenidos pertinentes y obligatorios

7.2 FACTORES ASOCIADOS A LOS PROCESOS

Los factores considerados asociados a los procesos son:

- **Diseño del proceso:** Claridad en la descripción del objetivo y alcance del proceso.
- **Proveedores del proceso:** Reconocimiento de entradas y salidas 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:** Interrelación en los procedimientos que desarrollan los procesos.
- **Responsables del proceso:** Grado de autoridad y responsabilidad de los lideres frente al proceso.
- **Comunicación entre los procesos:** Efectividad en los flujos de información.

8. ANÁLISIS DE RIESGOS

Al efectuar el análisis de riesgos la Guía para la Administración del Riesgo y el diseño de controles en entidades públicas, versión 5 de diciembre de 2020, precisa que "se busca establecer la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto.[18]

Señala la guía que se debe determinar la probabilidad, entendiéndose esta como la posibilidad de ocurrencia del riesgo.

Criterios para definir el nivel de probabilidad Fuente:

	FRECUENCIA DE ACTIVIDAD	PROBABILIDAD
Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año.	20%
Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año.	40%
Media	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año.	60%
Alta	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5000 veces por año.	80%
Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año.	100%

Tomado de la Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 5 de diciembre de 2020

Precisa además la Guía que se debe determinar el impacto: "Para la construcción de la tabla de criterios se definen los impactos económicos y reputacionales como las variables principales.[19]

"Cuando se presenten ambos impactos para un riesgo, tanto económico como reputacional con diferentes niveles, se debe tomar el nivel más alto.[20]

	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.

[18] https://www.funcionpublica.gov.co/documents/28587410/34298398/2020-12-
[19] Ídem al anterior
[20] Ídem al anterior

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 de 500 SMLMV.	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país

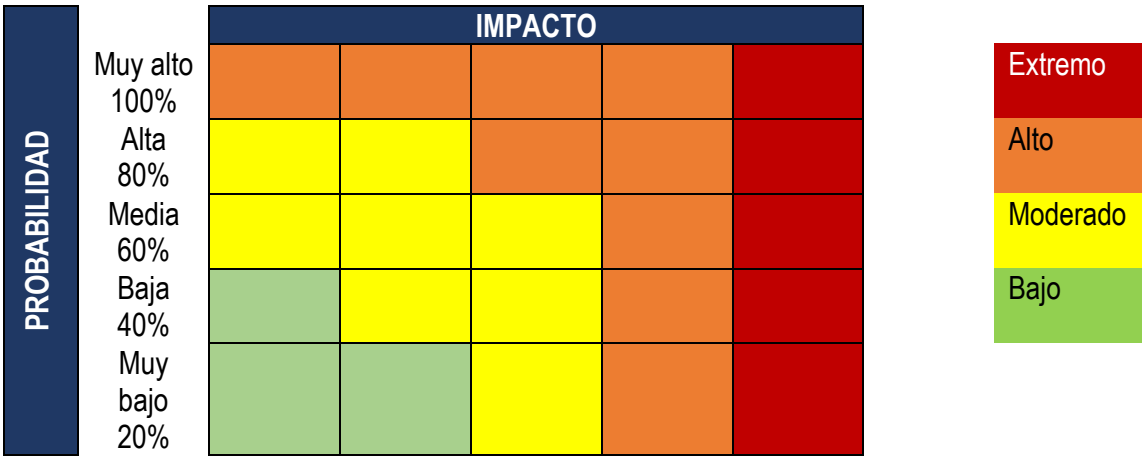
Tomado de la Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 5 de diciembre de 2020

9. EVALUACIÓN DE RIESGOS

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

9.1 Análisis preliminar (riesgo inherente)

Se trata de determinar los niveles de severidad a través de la combinación entre la probabilidad y el impacto. Se definen 4 zonas de severidad en la matriz de calor (ver figura 14). Figura 14 Matriz de calor (niveles de severidad del riesgo)[21]



Tomado de la Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 5 de diciembre de 2020

[21] Ídem al anterior

A partir de los criterios ERCA (Evitar, Reducir, Compartir y Asumir), la entidad establece los siguientes niveles de aceptación y periodicidad de seguimiento a los riesgos identificados:

- Cuando se mide la probabilidad e impacto de un riesgo residual de Proceso o Proyecto y este queda catalogado en nivel BAJO, se asumirá el riesgo y se administrará por medio de las actividades propias del proyecto o proceso asociado y su control y registro de avance se realizará en el reporte trimestral de su desempeño.
- Cuando el nivel del riesgo residual queda en MODERADO, se establecerán acciones de control preventivas que permitan REDUCIR la probabilidad de ocurrencia del riesgo, se administrarán mediante seguimiento trimestral y el líder del proceso dejará evidencias del seguimiento
- Cuando el nivel del riesgo residual queda ubicado en la zona de riesgo ALTA, se deberá incluir el riesgo tanto en el Mapa de Riesgo del Proceso como en el Mapa Empresarial de Riesgos y se establecerán acciones de Control Preventivas que permitan EVITAR la materialización del riesgo. La Administración de estos riesgos será con periodicidad al menos bimestral y el líder del proceso dejará evidencias de su adecuado control y seguimiento.
- Si el nivel del riesgo residual se ubica en la zona de riesgo CATASTRÓFICA, se incluirá el riesgo en el Mapa de Riesgo del Proceso y en el Mapa Empresarial de Riesgos, se establecerán acciones de control preventivas y correctivas que permitan EVITAR la materialización del riesgo. La Administración de estos riesgos será con periodicidad mínima MENSUAL y el líder del proceso dejará evidencias de su adecuado control y seguimiento. Adicionalmente se deberán documentar en el proceso, planes de contingencia para tratar el riesgo materializado, con criterios de oportunidad, evitando el menor daño en la prestación del servicio; estos estarán documentados en los planes de mejora de cada proceso.

9.2 Valoración de controles

De acuerdo a la Guía para la Administración del Riesgo, versión 5, esta es la estructura para la descripción del control: para una adecuada redacción del control se propone una estructura que facilitará más adelante entender su tipología y otros atributos para su valoración. La estructura es la siguiente:

- **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."[22]
- **Evidencia de la ejecución del control**
- **Tipo de control** (manual o automático)
- Cuando se realiza el control (periodicidad)
- La **valoración** del riesgo necesita de una evaluación de los controles existentes, lo cual exige determinar su naturaleza.

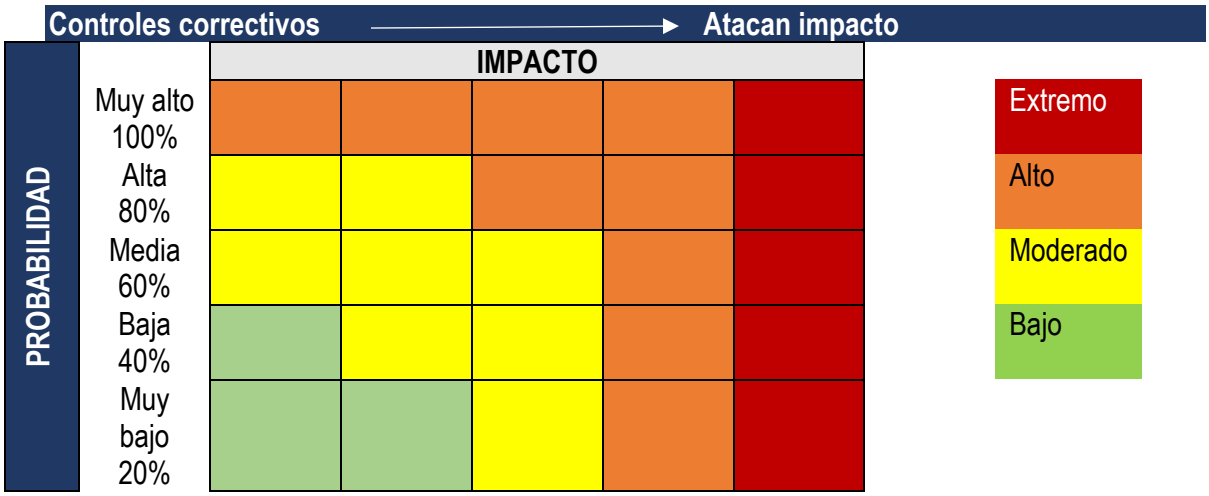
[22] Ídem al anterior

Si se trata de un control preventivo o correctivo, para este análisis se debe tener en cuenta:

- **Control Preventivo**: Evita que un evento suceda; por ejemplo, el requerimiento de un documento en un sistema de información es un control preventivo.
- "**Control detectivo:** control accionado durante la ejecución del proceso. Estos controles detectan el riesgo, pero generan reproceso."[23]
- **Control Correctivo:** No prevé que un evento suceda, pero permiten enfrentar la situación una vez se ha presentado; por ejemplo, en caso de un desastre natural u otra emergencia, mediante las pólizas de seguro y otros mecanismos de recuperación de los recursos.
- Si los **controles están documentados:** Evaluar cómo se lleva a cabo el control, quien es el responsable de su ejecución y cuál es la periodicidad para su ejecución, lo cual determinará las evidencias que van a respaldar la ejecución del mismo.

Si el control es:

- **Automático:** Utiliza herramientas tecnológicas como sistemas de información o software que permiten incluir contraseñas de acceso.
- **Manual:** Políticas de operación aplicables, autorizaciones a través de firmas o confirmaciones vía correo electrónico, archivos físicos, consecutivos, listas de chequeo.
- Determinar si se están aplicando en la actualidad y su efectividad.
- En la tabla ilustrativa, se muestran los criterios para la evaluación objetiva de los controles y determinar el desplazamiento dentro de la Matriz de Evaluación de Riesgos.



Tomado de la Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 5 de diciembre de 2020

[23] Ídem al anterior

Controles preventivos y detectivos → **Atacan probabilidad**

Atributos para el diseño de controles

Características			Descripción	Peso
Atributos de eficiencias	**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	Automáticos	Son actividades de procesamiento o validación de información que se ejecutan por un sistema y/o aplicativo de manera automática sin la intervención de personas para su realización.	25%
		Manual	Controles que son ejecutados por una persona, tiene implícito el error humano.	15%
Atributos informativos	**Documentación**	Documentado	Controles que están documentados en el proceso, ya sea en manuales, procedimientos, flujogramas o cualquier otro documento propio del proceso.	-
		Sin documentar	Identifica a los controles que pese a que se ejecutan en el proceso no se encuentran	-

			documentados en ningún documento propio del proceso	
	Frecuencia	Continua	El control se aplica siempre que se realiza la actividad que conlleva el riesgo	-
		Aleatoria	El control se aplica aleatoriamente a la actividad que conlleva el riesgo	-
	Evidencia	Con registro	El control deja un registro permite evidencia la ejecución del control.	-
		Sin registro	El control no deja registro de la ejecución del control.	-

Tomado de la Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 5 de diciembre de 2020

10. RIESGOS DE CORRUPCIÓN

La valoración de la probabilidad de ocurrencia de un riesgo de corrupción se debe llevar a cabo como lo señala el apartado No. 6 de esta política, es decir:

	FRECUENCIA DE ACTIVIDAD	PROBABILIDAD
Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año.	20%
Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año.	40%
Media	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año.	60%
Alta	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5000 veces por año.	801%
Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año.	100%

Tomado de la Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 5 de diciembre de 2020

Para la determinación del impacto frente a posibles materializaciones de riesgos de corrupción se analizarán únicamente los siguientes niveles i) moderado, ii) mayor, y iii) catastrófico, dado que estos riesgos siempre serán significativos, en tal sentido, no aplican los niveles de impacto insignificante y menor, que sí aplican para las demás tipologías de riesgos. Ahora bien, para establecer estos niveles de impacto se deberán aplicar las siguientes preguntas frente al riesgo identificado"[24].

Criterios para calificar el impacto del riesgo de corrupción:

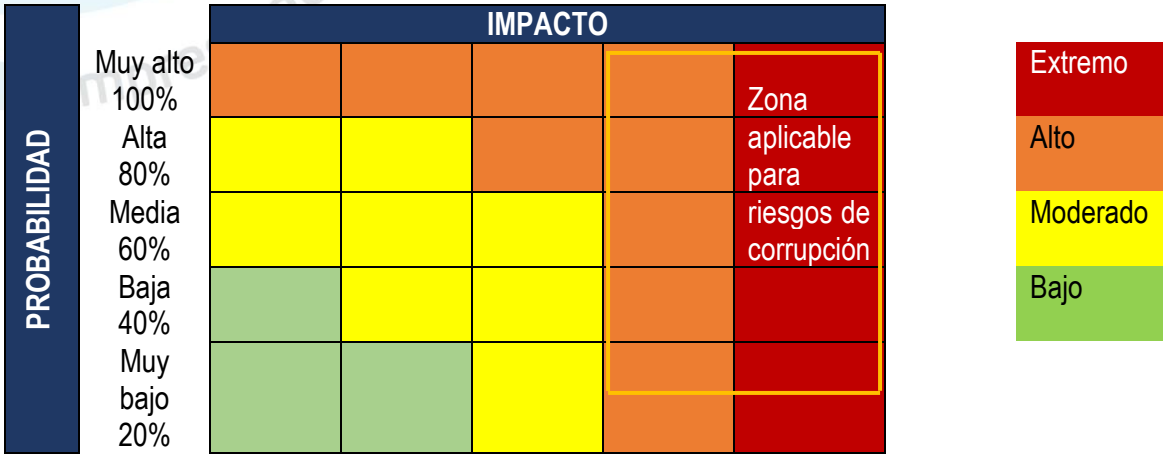
No.	Pregunta Si el riesgo de corrupción se materializa podría…	RESPUESTA	
		SÍ	NO
1	¿Afectar el grupo de funcionarios del proceso?		
2	¿Afectar el cumplimiento de metas y objetivos de la dependencia?		
3	¿Afectar el cumplimiento de misión de la entidad?		
4	¿Afectar el cumplimiento de la misión del sector al que pertenece la entidad?		
5	¿Generar pérdida de confianza de la entidad, afectando su reputación?		
6	¿Generar pérdidas de recursos económicos?		
7	¿Afectar la generación de los productos o la prestación del servicio?		
8	¿Dar lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien, servicios o 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 procesos sancionatorios?		
12	¿Dar lugar a procesos disciplinarios?		
13	¿Dar lugar a procesos fiscales?		
14	¿Dar lugar a procesos penales?		
15	¿Generar pérdida de credibilidad del sector?		
16	¿Ocasionar lesiones físicas o pérdidas de vidas humanas?		
17	¿Afectar la imagen regional?		
18	¿Afectar la imagen nacional?		
19	¿Generar daño ambiental?		
Responde afirmativamente de UNA a CINCO pregunta(s) genera un impacto moderado.			
Responde afirmativamente de SEIS a ONCE preguntas genera un impacto mayor.			
Responde afirmativamente de DOCE a DIECINUEVE preguntas genera un impacto catastrófico.[25]			

[24] Ídem al anterior

MODERADO	Genera medianas consecuencias sobre la entidad		
MAYOR	Genera altas consecuencias sobre la entidad.		

Tomado de la Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 5 de diciembre de 2020

Análisis preliminar (riesgo inherente): en esta etapa se define el nivel de severidad para el riesgo de corrupción identificado, para lo cual se aplica la matriz de calor establecida en el numeral 3.2.1 de la presente guía, teniendo en cuenta el ajuste frente a los niveles de impacto insignificante y menor mencionados en la determinación del impacto, lo que implica que las zonas de severidad para este tipo de riesgos se delimitan como se muestra a continuación:



Tomado de la Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 5 de diciembre de 2020

11. LINEAMIENTOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Estos lineamientos y esta parte del documento están basados en los planteamientos del Ministerio de Tecnologías de la información y las Telecomunicaciones y en la versión 5 de la Guía para la Administración del Riesgo. Teniendo en cuenta lo anterior, en primer lugar, se debe tener en cuenta que la política de seguridad digital se vincula al modelo de seguridad y privacidad de la información (MSPI), el cual se encuentra alineado con el marco de referencia de arquitectura TI y soporta transversalmente los otros habilitadores de la política de gobierno digital: seguridad de la información, arquitectura, servicios ciudadanos digitales.

11.1 Identificación de los activos de seguridad de la información

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

Conceptualización activos de información

¿Qué son los activos?	¿Por qué identificar los activos?
• Servicios web • Redes • Información física o digital • Tecnologías de información TI • Tecnologías de operación TO que utiliza la organización para funcionar en el entorno digital	La entidad puede saber **qué es lo que debe proteger para garantizar tanto su funcionamiento interno como su funcionamiento de cara al ciudadano**, aumentando así su confianza en el uso del entorno digital.
	La entidad puede saber **qué es lo que debe proteger para garantizar tanto su funcionamiento interno como su funcionamiento de cara al ciudadano**, aumentando así su confianza en el uso del entorno digital.

Fuente: Actualizado por la Dirección de Gestión y Desempeño Institucional de Función Pública y Ministerio TIC, 2020

11.2. Identificación del riesgo

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

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

Para cada riesgo se deben asociar el grupo de activos, o activos específicos del proceso, y conjuntamente analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización. Para este efecto, es necesario consultar el Anexo 4 Modelo nacional de gestión de riesgos de seguridad de la información para entidades públicas. donde se encuentran las siguientes tablas necesarias para este análisis:

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

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

Tipo de activos ejemplos de vulnerabilidades:

- Hardware
- Software Red Información
- Almacenamiento de medios sin protección
- Ausencia de parches de seguridad
- Líneas de comunicación sin protección
- Falta de controles de acceso físico
- Hurto de medios o documentos
- Abuso de los derechos Escucha encubierta Hurto de información

12. MAPA DE RIESGOS

Como producto final después de aplicar la metodología debe quedar el mapa de riesgos que es una representación final de la probabilidad e impacto de uno o más riesgos frente a un proceso, proyecto o programa.

13. MAPA INSTITUCIONAL DE RIESGO

Contiene a nivel estratégico los mayores riesgos a los cuales está expuesta la Empresa; se alimenta con los riesgos residuales altos y extremos de cada uno de los procesos que pueden afectar el cumplimiento de la misión institucional y objetivos de la Empresa. En este mapa se deberán incluir todos los riesgos identificados como posibles actos de corrupción, en cumplimiento del artículo 73 de la Ley 1474 de 2011.

14. MAPA DE RIESGOS POR PROCESO O PROYECTO

Recoge los riesgos identificados para cada uno de los procesos, los cuales pueden afectar el logro de sus objetivos.

Un mapa de riesgos se puede presentar como un consolidado donde se totalizan los riesgos y como una matriz o mapa de riesgos por proceso; Igualmente puede ser un mapa integrado (de gestión y de corrupción) como lo muestran los gráficos siguientes.

15. CONSIDERACIONES FINALES

La selección de los controles implica equilibrar los costos y los esfuerzos para su implementación, así como los beneficios finales, por lo tanto, se deberá considerar aspectos como:

- **Viabilidad Jurídica:** Velar por que los controles que se van a implementar no vayan en contra de la normatividad vigente.
- **Viabilidad técnica e institucional:** Establecer claramente si la entidad está en capacidad de implementar y sostener a largo plazo nuevas tecnologías u otros mecanismos necesarios para ejecutar el control.

- **Análisis costo-beneficio:** Prácticamente todas las respuestas a los riesgos implican algún tipo de costo directo o indirecto que se debe sopesar en relación con el beneficio que genera.

Una vez implementadas las acciones para el manejo de los riesgos, la valoración después de controles, se denomina RIESGO RESIDUAL, este se define como nivel de riesgo que permanece luego de tomar medidas de tratamiento al riesgo inherente.

BIBLIOGRAFÍA

- Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 5 de diciembre de 2020.
- Manual Operativo del Modelo Integrado de Planeación y Gestión, versión 4, marzo de 2021.
- Presidencia de la República, Estrategias para la Construcción del Plan Anticorrupción y de Atención al Ciudadano v2-2015
- Presidencia de la República, Guía para la gestión del riesgo de corrupción 2015.
- ESO, Documento Planeación Estratégica 2021-2025.
- EDESO, documento Política de Administración de riesgos