UNIDAD DE SERVICIOS PENITENCIARIOS Y CARCELARIOS - USPEC

POLÍTICA DE ADMINISTRACIÓN DE RIESGOS

BOGOTÁ D.C. MARZO 2022

USPEC
UNIDAD DE SERVICIOS
PENITENCIARIOS Y CARCELARIOS

Contenido

1. PROCESO

Gestión Estratégica Organizacional.

2. OBJETIVO

Establecer los lineamientos para la identificación, análisis, evaluación, tratamiento, monitoreo, revisión, y seguimiento de los riesgos de gestión, de corrupción y de seguridad de la información definidos en los procesos institucionales, con el fin de prevenir de forma anticipada su ocurrencia y minimizar el impacto y para el caso de riesgo de corrupción, sorteando la afectación del logro de los objetivos estratégicos y a su vez la misión de la Entidad.

3. ALCANCE

Comprende desde el análisis del contexto de la Entidad hasta la valoración y seguimiento tanto de los riesgos como de los controles establecidos en cada uno de los procesos de la Unidad de Servicios Penitenciarios y Carcelarios - USPEC. Incluye riesgos de gestión, corrupción y seguridad de la información.

4. DEFINICIONES

- **Activo:** son los elementos que tienen valor para la organización identificadas por cada proceso, tienen niveles de criticidad respectó a su confidencialidad, completitud e integridad, y cada jefe de área o jefe de oficina es el responsable del activo. Algunos de los activos que hay son: Aplicaciones de la organización, datos, archivos, servidores web, aplicaciones, servicios web, redes, Información física, digital, tecnologías de información, tecnologías de operación, personal, organización, hardware, software, red, información, bases de datos de nómina, aplicativo de nómina, cuentas de cobro. 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.

- **Análisis de riesgos:** proceso sistemático para entender la naturaleza del riesgo y evaluar la criticidad de reducir el nivel del riesgo.

- **Apetito de riesgo:** es el nivel de riesgo que la entidad puede aceptar en relación 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.

- **Capacidad de riesgo:** es el máximo valor del nivel de riesgo que una entidad puede soportar y a partir del cual la alta dirección considera que no sería posible el logro de los objetivos de la entidad.

- **Causa:** 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 las cuales se puede presentar el riesgo.
- **Confidencialidad**: propiedad de la información que la hace no disponible o sea 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.
- **Control:** medida que permite reducir o mitigar un riesgo.
- **Disponibilidad**: propiedad de la información de estar accesible y utilizable a demanda por una entidad.
- **Evaluación del control:** revisión sistemática de los procesos para garantizar que los controles aún son eficaces y adecuados.
- **Evaluación del riesgo:** proceso de comparar el nivel de riesgo frente a los criterios del riesgo.
- **Evitar el riesgo:** decisión de no involucrarse en o retirarse de una situación de riesgo**.**
- **Factores de riesgo**: son las fuentes generadoras de riesgos.
- **Frecuencia:** medición del número de ocurrencias por unidad de tiempo.
- **Gestión del Riesgo:** un 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.
- **Impacto**: las consecuencias que puede ocasionar a la organización la materialización del riesgo.
- **Integridad:** propiedad de la información relativa a su exactitud y completitud.
- **Nivel de riesgo:** es el valor que se determina a partir de combinar la probabilidad de ocurrencia de un evento potencialmente dañino y la magnitud del impacto que este evento traería sobre la capacidad institucional de alcanzar los objetivos. En general la fórmula del nivel del riesgo puede ser Probabilidad * Impacto, sin embargo, pueden relacionarse las variables a través de otras maneras diferentes a la multiplicación, por ejemplo, mediante una matriz de Probabilidad –Impacto.
- **Mapa de riesgos:** herramienta metodológica que permite hacer un inventario de los riesgos detallando la descripción de cada uno de éstos y las posibles consecuencias.
- **Monitorear:** verificar, supervisar, observar críticamente o medir regularmente el progreso de una actividad, una acción o un sistema para identificar los cambios en el nivel de desempeño requerido o esperado.
- **Política de administración de riesgos:** declaración de la dirección y las intenciones de una organización con respecto a la gestión del riesgo. La gestión o administración del riesgo establece lineamientos precisos acerca del tratamiento; manejo y seguimiento a los riesgos. Es establecida por la dirección de la entidad, con la participación del comité institucional

- **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.

- **Plan de manejo o tratamiento del riesgo:** plan de acción propuesto por el grupo de trabajo.

- **Reducción del riesgo:** acciones que se toman para disminuir la posibilidad, las consecuencias negativas, o ambas, asociadas con un riesgo.

- **Responsables:** son las dependencias o áreas encargadas de adelantar las acciones propuestas.

- **Riesgo:** efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales. Nota: lo 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.

- **Riesgo de seguridad de la información**: posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000)

- **Riesgo de corrupción:** posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.

- **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.

- **Seguimiento:** recolección regular y sistemática sobre la ejecución del plan, qué sirven para actualizar y mejorar la planeación futura.

- **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.

- **Valoración del riesgo:** proceso total de identificación del riesgo, análisis del riesgo 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. DISPOSICIONES GENERALES

Este documento describe la metodología y establece los lineamientos para la administración de los riesgos de gestión, corrupción y seguridad de la información para la Unidad de Servicios Penitenciarios y Carcelarios - USPEC, y adopta la Guía para la Administración del Riesgo del Departamento Administrativo de la Función Pública - DAFP.

- Los lineamientos de la política de administración de riesgos de la USPEC son establecidos por la Alta Dirección en cabeza de la Dirección General, y con la participación del Comité Institucional de Coordinación de Control Interno.

- La identificación de riesgos y su actualización deben tener en cuenta como insumo la misión, visión, objetivos estratégicos, metas, planes, proyectos y las prioridades de la Entidad, incluyendo las del plan de desarrollo vigente. Adicionalmente, se debe tener en cuenta el contexto organizacional, caracterizaciones de los procesos, informes de entes de control y de la Oficina de Control Interno.

- La identificación, análisis, valoración y administración de los riesgos (gestión, corrupción y seguridad de la información) debe realizarse a todos los procesos.

- Para el levantamiento, actualización y seguimiento de los riesgos de gestión, corrupción y de seguridad de la información se debe utilizar la Herramienta de Administración de Riesgos.

- Los riesgos de seguridad de la información, se deben gestionar de acuerdo con los criterios diferenciales descritos en el modelo de seguridad y privacidad de la información.

- Los riesgos (gestión, corrupción y seguridad de la información) deben ser elaborados y/o revisados anualmente por los responsables de procesos y su equipo, antes del inicio de cada vigencia.

- La identificación o actualización de activos de información se debe realizar teniendo en cuenta los lineamientos establecidos en el Manual de Clasificación de Activos.

- Los riesgos de seguridad de la información se analizarán para aquellos activos valorados como "Críticos" y "Altos".

6. RESPONSABILIDADES

6.1 RESPONSABILIDAD DE LA LÍNEA ESTRATÉGICA (Alta Dirección y Comité Institucional de Control Interno)

- Definir y aprobar los lineamientos para la gestión del riesgo y el control, y supervisar su cumplimiento en acompañamiento del Comité Institucional de Coordinación de Control Interno.

- Revisar los cambios que se generen en el contexto de la Entidad y que puedan desplegar nuevos riesgos o modificación de los ya identificados.

- A través del Comité Institucional de Control Interno realizar seguimiento a la gestión del riesgo y a los resultados de las evaluaciones que realiza la Oficina de Control Interno y de auditorías internas.

- Tener en cuenta los incidentes de seguridad digital que hayan afectado a la Entidad, para la toma de decisiones en el proceso de revisión de los riesgos.

6.2 RESPONSABILIDAD DE LA PRIMERA LÍNEA DE DEFENSA (líderes de proceso y de proyectos)

- Identificar, valorar y actualizar cuando sea necesario, los riesgos que puedan afectar los planes, proyectos y procesos a su cargo, enfatizando en la prevención del daño antijurídico.

- Definir, implementar y monitorear los controles para mitigar los riesgos identificados, y que contribuyan al cumplimiento de las metas y objetivos de la Entidad. Detectar las deficiencias de los controles y establecer las acciones de mejora correspondientes.

- Informar a la Oficina Asesora de Planeación y Desarrollo, y a la Dirección General, cuando se presente la materialización de riesgos en los planes, proyectos o procesos a su cargo.

- Reportar los avances y evidencias de la gestión de los riesgos a cargo.

- Realizar seguimiento cada tres meses a los riesgos en la Herramienta de Administración de Riesgos", y reportarlo a la Oficina Asesora de Planeación y Desarrollo y a la Oficina de Control Interno con las evidencias correspondientes de la gestión.

- Revisar los riesgos del proceso durante el último trimestre de cada año, para su actualización, aprobación y publicación en el portal web institucional máximo el 31 de enero de la siguiente vigencia.

- Elaborar e implementar políticas y procedimientos internos asegurando que sean compatibles con las metas y objetivos de la USPEC, emprendiendo acciones de mejora para su logro.

6.2.1 RESPONSABILIDAD DE LA SEGUNDA LÍNEA DE DEFENSA (Oficina Asesora de Planeación y Desarrollo, responsables de sistemas de gestión)

- Liderar el proceso de administración de los riesgos y consolidar el mapa de riesgos institucional (riesgos de mayor criticidad y/o relevantes frente al logro de los objetivos).

- Acompañar, orientar y entrenar a los líderes de procesos en la identificación, análisis y valoración del riesgo.

- Dar a conocer a funcionarios y contratistas el mapa de riesgos antes de su publicación. De igual manera se debe dar a conocer a la ciudadanía y partes interesadas (población objeto identificada). Se deben conservar las evidencias de la socialización, así como consolidar y publicar los aportes recibidos.

- Publicar el mapa de riesgos máximo el 31 de enero de cada vigencia, en la sección de transparencia y acceso a la información.

- Definir condiciones de reserva y clasificación de elementos constitutivos del mapa de riesgos.

- Acompañar a los líderes de procesos en las modificaciones a los riesgos y dejar trazabilidad de las modificaciones realizadas.

- Monitorear la implementación de los controles definidos por la primera línea de defensa, teniendo en cuenta la información suministrada por los líderes de procesos.

- Evaluar que los riesgos identificados por la primera línea de defensa cumplan con los lineamientos definidos.

- Realizar monitoreo trimestral y consolidar los avances y actualizaciones al mapa de riesgos, y publicar en página web.

- Realizar divulgación y socialización de los mapas de riesgos por proceso y el Mapa de Riesgos Institucional aprobados, al interior de la Entidad.

- Informar a la línea estratégica sobre cualquier variación importante en los niveles o valoraciones de los riesgos de seguridad de la información.

Nota: Para los riesgos de seguridad de la información, el acompañamiento, seguimiento, monitoreo y consolidación lo realiza la Oficina de Tecnología, y remite las modificaciones y seguimientos a la Oficina Asesora de Planeación y Desarrollo.

6.2.2 RESPONSABILIDAD DE LA TERCERA LÍNEA DE DEFENSA (Oficina de Control Interno)

- Asesorar en coordinación con la Oficina Asesora de Planeación y Desarrollo y la Oficina de Tecnología, a la primera línea de defensa en la identificación, análisis y valoración del riesgo, y en el diseño de los controles.

- Verificar la publicación del mapa de riesgos en el portal web institucional.

- Realizar seguimiento a la gestión de riesgos (analizar causas, riesgos, eficacia y efectividad de los controles), en los procesos que realice de auditorías internas.

- Recomendar mejoras a la política de administración del riesgo.

- Realizar monitoreo y evaluación a la gestión de riesgos por lo menos dos veces al año, una por semestre.

- Realizar seguimiento a los riesgos de corrupción cada cuatro meses y publicarlo en la página web de la Entidad para consulta, de la siguiente manera:

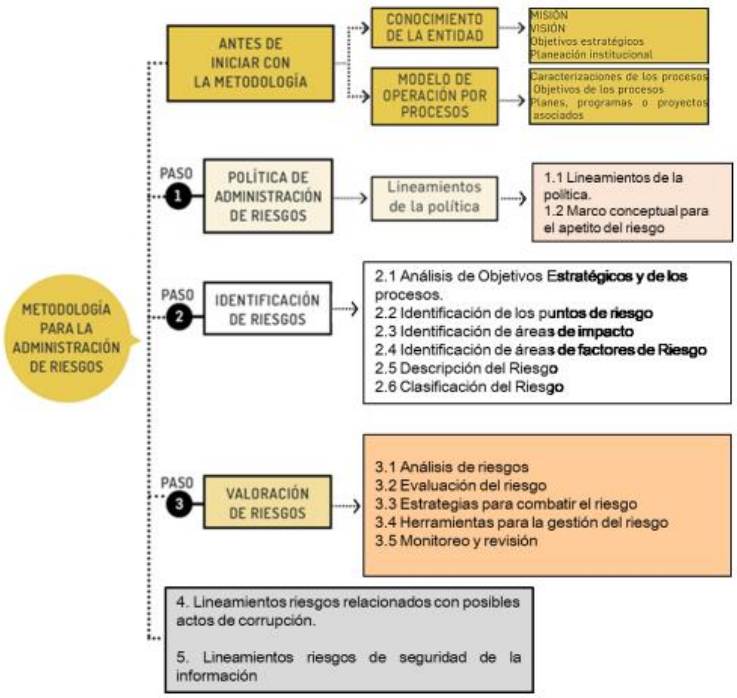
  Primer corte 30 de abril: se publica dentro de los diez (10) primeros días hábiles del mes de mayo.
  Segundo corte 31 de agosto: se publica dentro de los diez (10) primeros días hábiles del mes de septiembre.
  Tercer corte al 31 de diciembre: se publica dentro de los diez (10) primeros días hábiles del mes de enero.

7. METODOLOGÍA

Administración de Riesgos USPEC

La política de administración de riesgos se rige por las disposiciones legales y en particular por la Guía para la administración del riesgo y el diseño de controles en entidades públicas del Departamento Administrativo de la Función Pública (versión 2020) que establece las directrices de obligatorio cumplimiento para las entidades públicas.

Los riesgos en la USPEC se categorizan por procesos (Modelo de Operación por Procesos). Teniendo en cuenta que el adecuado manejo de los riesgos favorece el desarrollo y sostenibilidad de la gestión de la entidad, es importante que el líder del proceso (Directivos, entiéndase como él Director General, Directores, Subdirectores y Jefes de Oficina), a través de los formatos dispuestos en el Sistema Integrado de Gestión frente a este proceso, establezca la identificación, análisis, valoración y definición de las alternativas de acciones de mitigación de los riesgos.



Metodología para la Administración de Riesgos – Guía DAFP 2020

Nivel de Aceptación

Apetito de Riesgo/Tratamiento del Riesgo
Se considera el apetito del riesgo en la descripción de cada riesgo como su tolerancia aceptada.

La metodología para la identificación, análisis, evaluación, tratamiento, monitoreo, revisión y seguimiento de los riesgos de la Entidad, está basada en la "Guía para la administración del riesgo y el diseño de controles en entidades públicas" del DAFP, su "Anexo 4 Lineamientos para la gestión de riesgos de seguridad digital en entidades públicas" de MinTIC, o el documento que lo sustituya; para mayor detalle puede consultar el documento en la página web del DAFP. Los pasos y lineamientos específicos para la USPEC, son los siguientes:

Revisión previa a la aplicación de la metodología

- Revisión de la misión y la visión.
- Revisión de objetivos estratégicos.
- Los objetivos estratégicos deben estar alineados a la misión, visión y propósito superior.
- Los objetivos deben incluir el qué, cómo, para qué, cuándo, cuánto.
- Los objetivos definidos deben contemplar al menos las siguientes características: específico, medible, alcanzable, relevante y proyectado en el tiempo.
- Revisión de objetivos estratégico y del proceso: Le corresponde a la segunda línea de defensa la revisión de los objetivos de la Entidad tanto del orden estratégico como de procesos. Es decir, en la medida que se construyen los procesos, la Oficina Asesora de Planeación entre sus funciones de calidad realiza las

recomendaciones y/o sugerencias pertinentes con el fin de que los objetivos institucionales y de procesos se encuentren bien definidos.

- Análisis de objetivos de los procesos: Al menos se deben analizar qué cumplan con las características mencionadas anteriormente y asegurar que contribuyan a los objetivos estratégicos.

Contexto del proceso.

La base y el principal documento para identificar el contexto del proceso es su caracterización, por medio del cual se estructuran los procesos y subprocesos estableciendo su objetivo, alcance, recursos, proveedor, entradas o insumos su transformación a través de las actividades y procedimientos salidas o productos, clientes y los indicadores para garantizar su control.

Para realizar el análisis del contexto externo e interno del proceso se debe identificar el propósito y la dirección estratégica, a partir del conocimiento de las situaciones del entorno de la Entidad, tanto de carácter social, económico, cultural, ambiental, tecnológico, ambiental, entre otros y en qué pueden afectar las capacidades para lograr los resultados. El líder del proceso con su equipo de trabajo debe revisar los lineamientos del Plan Estratégico de la Entidad

7.1 IDENTIFICACIÓN DE RIESGOS

Previo a la identificación de los riesgos, la Oficina Asesora de Planeación y Desarrollo debe revisar los objetivos estratégicos y los objetivos de los procesos; debe validar que los objetivos en su descripción o redacción den respuesta a las siguientes preguntas: ¿qué se quiere lograr?, ¿para qué quiere lograrlo?, ¿cómo quiere lograrlo?, ¿cuándo piensa lograrlo? y ¿cuánto avance debo cumplir en cada vigencia?

La identificación del riesgo se debe registrar en la hoja “Identificación riesgo” de la “Herramienta de Administración de Riesgos”.

7.1.1 Establecimiento del contexto

Se debe identificar los riesgos que estén o no bajo el control de la USPEC, teniendo en cuenta el contexto estratégico en el que opera la Entidad, la caracterización de procesos contemplando su objetivo y alcance

Los líderes de procesos deben establecer el contexto interno y externo de la Entidad, el contexto de los procesos y los activos de seguridad digital. Los factores para cada categoría son:

FACTORES	
CONTEXTO EXTERNO	POLÍTICOS: cambios de gobierno, legislación, políticas públicas, regulación.
	ECONÓMICOS Y FINANCIEROS: disponibilidad de capital, liquidez, mercados financieros, desempleo, competencia.
	SOCIALES Y CULTURALES: demografía, responsabilidad social, orden público.
	TECNOLÓGICOS: avances en tecnología, acceso a sistemas de información externos, gobierno en línea.
	AMBIENTALES: emisiones y residuos, energía, catástrofes naturales, desarrollo sostenible.

	LEGALES Y REGLAMENTARIOS: Normatividad externa (leyes, decretos, ordenanzas y acuerdos).
CONTEXTO INTERNO	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.
	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	DISEÑO DEL PROCESO: claridad en la descripción del alcance y objetivo del proceso.
	INTERACCIONES CON OTROS PROCESOS: relación precisa con otros procesos en cuanto a insumos, proveedores, productos, usuarios o clientes.
	TRANSVERSALIDAD: procesos que determinan lineamientos necesarios para el desarrollo de todos los procesos de la entidad.
	PROCEDIMIENTOS ASOCIADOS: pertinencia en los procedimientos que desarrollan los procesos.
	RESPONSABLES DEL PROCESO: grado de autoridad y responsabilidad de los funcionarios frente al proceso.
	COMUNICACIÓN ENTRE LOS PROCESOS: efectividad en los flujos de información determinados en la interacción de los procesos.
	ACTIVOS DE SEGURIDAD DIGITAL DEL PROCESO: información, aplicaciones, hardware entre otros, que se deben proteger para garantizar el funcionamiento interno de cada proceso, como de cara al ciudadano.

7.1.2 Identificación del riesgo

Luego de establecer el contexto (incluyendo causas y consecuencias) se deben identificar los riesgos, que son aquellos eventos o situaciones que pueden llegar a entorpecer el normal desarrollo de los objetivos del proceso o los estratégicos. Para ello, es necesario responder las siguientes preguntas para la identificación: ¿qué puede suceder?, ¿Cómo puede suceder?, ¿Cuándo puede suceder? y ¿Qué consecuencias tendría su materialización?, y con las respuestas construir la descripción del riesgo.

Luego se deben identificar las causas del riesgo que pueden afectar el logro de los objetivos y las consecuencias o efectos resultantes de la materialización de un riesgo que afecte los objetivos del proceso, la entidad o partes interesadas. También, se deben identificar las amenazas y vulnerabilidades de los activos de información que generen

riesgos de seguridad digital. Se debe tener conocimiento general del proceso y tener acceso o conocimiento de datos y hechos históricos de la Entidad para realizar una completa identificación.

Para la identificación de los activos de información es necesario considerar los lineamientos establecidos en el "Manual de Clasificación de Activos".

En la descripción de riesgos de corrupción, es preciso atender al cumplimiento de los siguientes componentes: Acción u omisión + uso del poder + desviación de la gestión de lo público + el beneficio privado. La descripción del riesgo debe ser clara y precisa, además para clasificarse como riesgo de corrupción debe cumplir con las cuatro condiciones.

Para cada riesgo de seguridad digital se deben vincular los activos relacionados y se deben evaluar amenazas y vulnerabilidades que pueden causar la materialización del riesgo. Se pueden identificar tres riesgos de seguridad digital:

- Pérdida de confidencialidad.
- Pérdida de integridad.
- Pérdida de disponibilidad.

7.2 VALORACIÓN DE RIESGOS (análisis y evaluación)

En esta fase se define la probabilidad de ocurrencia del riesgo (eventos positivos y/o negativos) y su consecuencia o impacto para estimar la zona de riesgo inicial (riesgo inherente antes del diseño de controles), y luego comparar los resultados frente a los controles diseñados y evaluados, para determinar la zona de riesgo final (riesgo residual) y estipular de acuerdo con las capacidades de la Entidad su aceptación y tratamiento.

7.2.1 Análisis de riesgos

El objetivo es analizar la posibilidad de ocurrencia del riesgo y expresarla en términos de frecuencia (hechos que se han materializado) o factibilidad (hechos que no se han presentado pero es posible que suceda). Los criterios para calificar la probabilidad son:

El análisis del riesgo busca establecer la probabilidad de ocurrencia de los riesgos así como el impacto de sus consecuencias, calificándolos y evaluándolos con el fin de obtener información para establecer el nivel de riesgo, también las acciones que se van a implementar. En el análisis del riesgo se deberán considerar los aspectos de Calificación y Evaluación del riesgo; además dependerá de la información obtenida de la identificación de riesgos, incluso la disponibilidad de datos históricos y aportes de los servidores de la organización.

Se deben contemplar dos aspectos en el análisis de los riesgos identificados: Probabilidad e Impacto.

Por probabilidad se entiende la posibilidad de ocurrencia del riesgo; esta puede ser medida con criterios de frecuencia si se ha materializado, o de factibilidad teniendo en cuenta la presencia de factores internos y externos que puedan propiciar el riesgo aunque este no se haya materializado

Por impacto se entienden las consecuencias que puede ocasionar a la organización la materialización del riesgo.

Para adelantar el análisis del riesgo se deben considerar los siguientes aspectos:

- Calificación del riesgo: se logra a través de la estimación de la probabilidad de su ocurrencia y el impacto que puede causar la materialización del riesgo.

- Bajo el criterio de probabilidad: el riesgo se debe medir a partir de las siguientes especificaciones:

Tabla de Probabilidad

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

- Bajo el criterio de impacto, el riesgo se debe medir a partir de las siguientes especificaciones:

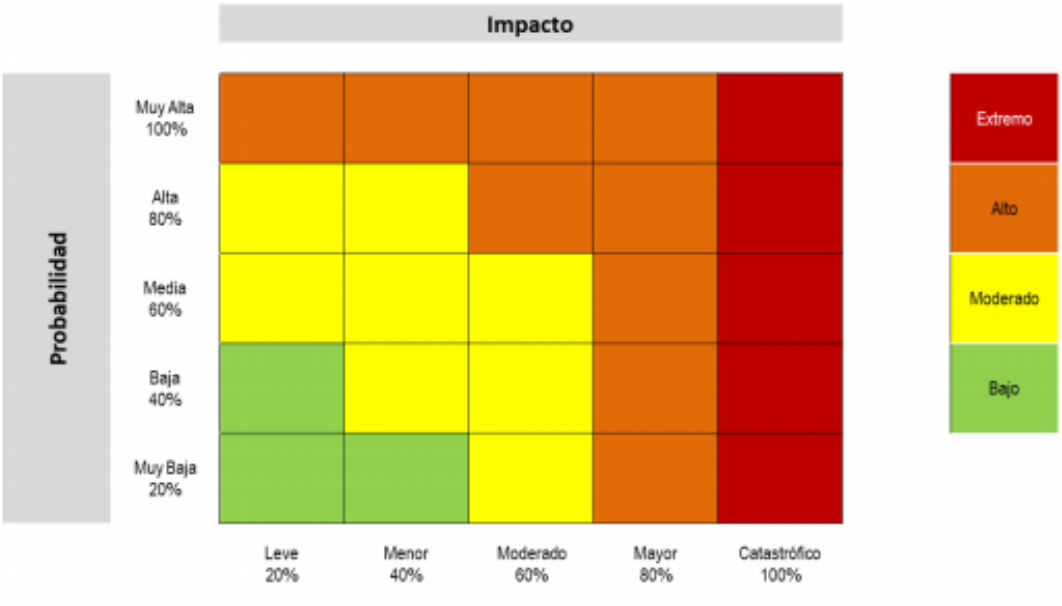
	Afectación Económica	Reputacional
Leve 20%	Afectación menor a 10 SMLMV .	El riesgo afecta la imagen de algún área de la organización.
Menor-40%	Entre 10 y 50 SMLMV	El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, de junta directiva y accionistas y/o de proveedores.
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 500SMLMV, el impacto del riesgo es **mayor**.

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

Los criterios para calificar el impacto para los riesgos de gestión, corrupción y seguridad digital, se encuentran vinculados en la Herramienta de Administración de Riesgos.

Con el resultado de la calificación del riesgo, se ubica el impacto y probabilidad en el mapa de calor, para determinar el nivel de riesgo, y como resultado se obtiene el ***riesgo inherente***:



Extremo	Reducir el riesgo, Evitar, Compartir o Transferir.
Alto	Reducir el riesgo, Evitar, Compartir o Transferir.
Moderado	Asumir el Riesgo, Reducir el Riesgo.
Bajo	Asumir el Riesgo.

Nota:
Para los riesgos de corrupción solo aplican las columnas de Impacto Moderado, Mayor y Catastrófico.

7.2.2 Evaluación de riesgos

Para esto es necesario diseñar los controles para mitigar de manera adecuada el riesgo. La descripción del control debe contener las variables incluidas en la Herramienta de Administración de Riesgos (hoja "Valoración riesgos"): responsable, periodicidad, propósito, cómo se realiza, qué pasa con las observaciones o desviaciones, y evidencia. Para cada causa debe existir un control.

Luego del diseño de los controles, se debe valorar si está bien diseñado para mitigar el riesgo y si se ejecuta como fue diseñado y es consistente.

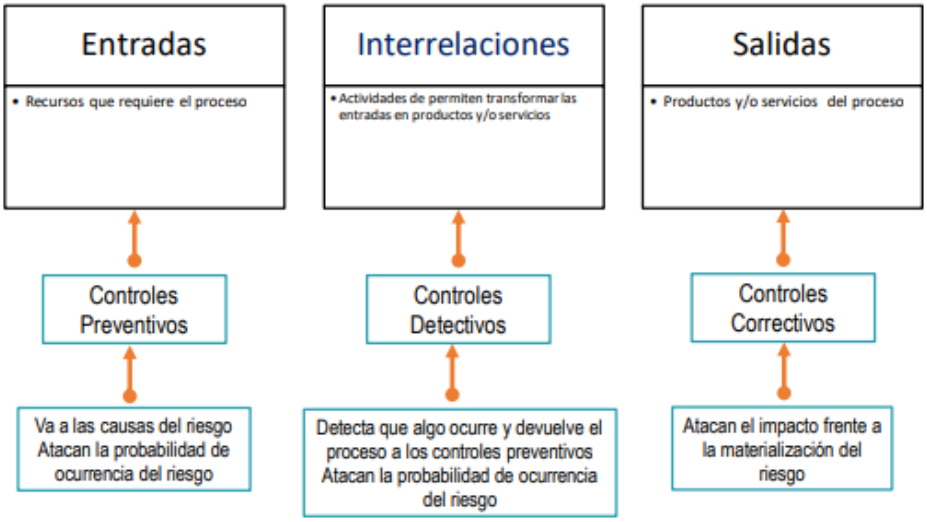
Nota: Ningún riesgo con medida de tratamiento se evita o elimina.

Finalmente, de acuerdo con los resultados de la evaluación realizada a la solidez del conjunto de los controles, se debe determinar el desplazamiento del riesgo en el mapa de calor, si disminuyen la probabilidad o el impacto. Para el caso de riesgos de corrupción únicamente disminuye la probabilidad, no debe haber desplazamiento en el impacto.
La valoración del riesgo es el producto de confrontar los resultados de la evaluación del riesgo con los controles identificados, esto se hace con el objetivo de establecer prioridades para su manejo y para la fijación de políticas. Para adelantar esta etapa se hace necesario tener claridad sobre los puntos de control existentes en los diferentes procesos, los cuales permiten obtener información para efectos de tomar decisiones.

Los controles deben tener relación directa con las causas generadoras del riesgo identificado, para ello es importante revisar que las actividades de control subsanen y/o prevengan los agentes generadores del riesgo identificado. Así mismo, es importante considerar las acciones de manera correctiva que se puedan adelantar para mitigar los efectos de un riesgo cuando se ha materializado.

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

Figura 16 Ciclo del proceso y las tipologías de controles



Algunos ejemplos de tipos de control se presentan a continuación:

Controles de Gestión	Políticas claras aplicadas
	Seguimiento al plan estratégico y operativo
	Indicadores de gestión
	Tableros de control
	Seguimiento al cronograma
	Evaluación del desempeño
	Informes de gestión
	Monitoreo de riesgos
Controles operativos	Conciliaciones
	Consecutivos
	Verificación de firmas
	Listas de chequeo
	Registro controlado
	Segregación de funciones
	Niveles de autorización
	Custodia apropiada
	Procedimientos formales aplicados
	Pólizas
	Seguridad física
	Contingencias y respaldo
	Personal capacitado
	Aseguramiento y calidad
Controles legales	Normas claras
	Control de términos

Es importante revisar que los controles documentados son actividades recurrentes o periódicas. Existen tres tipos de controles, en cuanto al efecto sobre el riesgo:

- **Preventivos:** son aquellas acciones encaminadas a eliminar las causas generadoras de un riesgo, de tal manera que eviten o disminuyan su ocurrencia o materialización

- **Detectivos:** control accionado durante la ejecución del proceso. Estos controles detectan el riesgo, pero generan reprocesos

- **Correctivos:** son aquellas acciones que permiten el restablecimiento de la actividad, después de ser detectado un evento no deseable. A través de estos controles se puede cambiar o modificar las acciones que propiciaron su ocurrencia y corregir los productos o servicios generados de la actividad crítica antes de ser suministrados al cliente.

El procedimiento para la valoración del riesgo parte de la evaluación de los controles existentes, lo cual implica:

Describirlos (estableciendo si son preventivos o correctivos)
Revisarlos para determinar si los controles están documentados, si se están aplicando en la actualidad y si han sido efectivos para minimizar el riesgo
Es importante que la valoración de los controles incluya un análisis de tipo cuantitativo, que permita saber con exactitud cuántas posiciones dentro de la matriz de calificación, evaluación y respuesta al riesgo

¿Cómo se valoran los controles?

Con las siguientes herramientas se podrán ponderar de manera objetiva los controles y poder determinar el desplazamiento dentro de la Matriz de Calificación, Evaluación y Respuesta a los riesgos

Diseño 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.

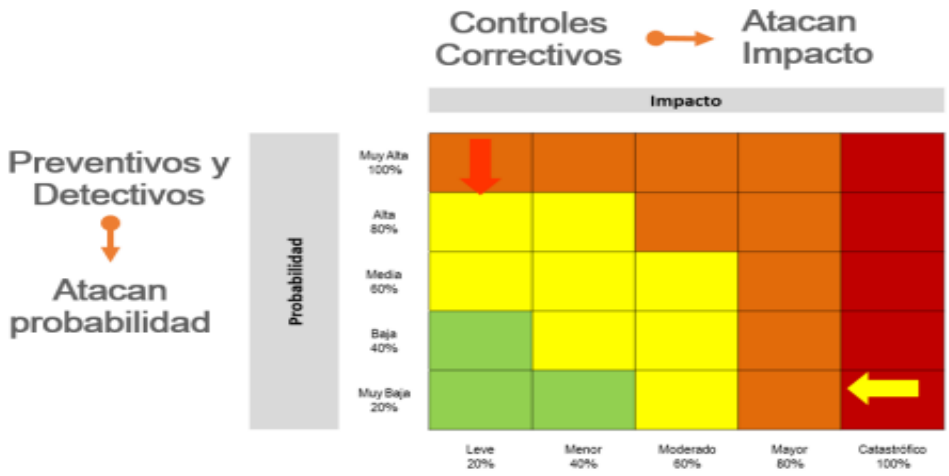
En la siguiente tabla se puede observar la descripción y peso asociados a cada uno así:

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	

Características			Descripción	Peso
			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.	
		Aletoria	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.	

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.

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.



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

7.2.3 Tratamiento del riesgo

La primera línea de defensa es la responsable de definir las acciones de tratamiento para mitigar los riesgos identificados (Plan de Tratamiento de Riesgos). Para los riesgos de corrupción las opciones de tratamiento después de la valoración de controles solo deben ser: evitar, compartir o reducir el riesgo.

Todos los riesgos con evaluación después de controles que se encuentren en zona “Alta” y “Extrema”, deben definir acciones para el tratamiento de los riesgos. Las opciones de tratamiento y los lineamientos para cada uno son:

- **Aceptar el riesgo:** no se adopta ninguna medida que afecte la probabilidad o el impacto del riesgo. Esto debe aplicar para riesgos inherentes calificados como “bajo” ya que no es necesario poner controles o no es posible aplicar controles. Para esta opción de tratamiento se debe realizar seguimiento continuo al riesgo *(Ningún riesgo de corrupción debe ser aceptado)*.

- **Reducir el riesgo:** se adoptan medidas para reducir la probabilidad o el impacto del riesgo, o ambos; por lo general conlleva a la implementación de controles.

- **Evitar el riesgo:** se abandonan las actividades que dan lugar al riesgo, es decir, no dar inicio o no continuar con la actividad que lo provoca.

- **Compartir el riesgo:** se reduce la probabilidad o el impacto del riesgo transfiriendo o compartiendo una parte de este. Los riesgos de corrupción se pueden compartir pero no transferir su responsabilidad. Las opciones más utilizadas para esta situación es que la Entidad adquiera seguros y/o realice la tercerización que aumenta la probabilidad del riesgo, y en caso de decidir esta opción de tratamiento, debe estar formalizada a través de un acuerdo contractual

Para tratar o mitigar los riesgos de seguridad digital, se deben tomar como referencia los controles establecidos en el Anexo A de la Norma ISO 27001:2013. Una vez se implementen estos controles, debe actualizarse el documento que contiene la declaración de aplicabilidad de la Entidad, con el fin de incluir en cada control los soportes de su implementación. Esta tarea está a cargo del responsable de riesgos en seguridad digital de la Entidad.
Es preciso definir actividades de control para prevenir que el riesgo se materialice, y si llega a pasar, debe ser detectado de manera oportuna. Los tipos de controles son:

- Preventivos: diseñados para evitar la ocurrencia de riesgos que afecten el cumplimiento de los objetivos.

- Detectivos: diseñados para detectar la situación no deseada, se corrija y se tomen las acciones correspondientes.

- Correctivos: diseñados para atacar el impacto frente a la materialización del riesgo.

Los mapas de riesgos, que incluyen Planes de Tratamiento de Riesgos y la aceptación de los riesgos residuales, deben ser aprobados por los líderes de proceso a través de acta o correo electrónico.

Después de definidos los mapas de riesgos de todos los procesos, la Oficina Asesora de Planeación y Desarrollo debe consolidar y generar el mapa de riesgos Institucional, el cual debe contener los riesgos de gestión, corrupción y seguridad digital. El mapa debe ser aprobado en Comité Institucional de Control Interno, para su posterior socialización y publicación.

7.3 MONITOREO Y REVISIÓN

- El Mapa de riesgos de proceso, debe contener aquellas acciones de control definidas para el manejo del riesgo, buscando prevenir o reducir el riesgo detectado, teniendo en cuenta su viabilidad técnica y financiera. El monitoreo de las acciones de tratamiento debe realizarlo el responsable del proceso.

- El responsable del proceso deben verificar que los controles establecidos en el plan de tratamiento de riesgos operen de manera adecuada para mitigar los riesgos.

- El seguimiento de los riesgos identificados (incluyendo el plan de tratamiento) se debe realizar de manera trimestral por cada uno de los líderes de los procesos, quienes reportarán a la Oficina Asesora de Planeación y Desarrollo (Riesgos de Gestión y Corrupción) y la Oficina de Tecnología (Riesgos de Seguridad Digital) los avances en las acciones y las evidencias correspondientes en la “Herramienta de Administración de Riesgos”.

- En caso de materialización de un riesgo, el responsable del proceso debe generar una acción correctiva, y debe revisar nuevamente la identificación del riesgo, el diseño y valoración de controles, y el plan de tratamiento para mitigar el riesgo.

- Anualmente se debe realizar la valoración de los riesgos de gestión, corrupción y seguridad digital con el fin de verificar que los planes de tratamiento fueron efectivos y los niveles de riesgo disminuyeron.

- El responsable realizar el seguimiento a los riesgos de seguridad digital debe reportar semestralmente a la Dirección General el estado de los mismos.

RESUMEN DE CAMBIOS

Versión	Fecha	Numerales	Descripción de la modificación
01	28/04/2015	Todos	Se crea el documento
02	10/03/2016	Todos	Se actualizan todos los numerales del documento y se introducen los lineamientos Institucionales para la gestión del riesgo de corrupción
03	17/10/2019	Todos	Se actualizan todos los numerales acorde a la Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 4, 2018.
	04/10/2021	5, 6 y 7	Se ajustan los códigos de los documentos de acuerdo con la actualización del Mapa de Procesos Institucional. La versión del documento se mantiene debido a que su contenido no se modificó.
04	31/03/2022	Todos	Se actualizan todos los numerales acorde a la Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 5, 2020.

RESPONSABILIDAD Y AUTORIDAD		
Elaboró / Actualizó:	**Revisó:**	**Aprobó:**
Nombre: Jenny Marcela Mesa	Nombre: Marisol Villamil Morales	Nombre: Marisol Villamil Morales
Cargo: Contratista	Cargo: Jefe Oficina	Cargo: Jefe Oficina
Dependencia: Oficina Asesora de Planeación y Desarrollo.	Dependencia: Oficina Asesora de Planeación y Desarrollo.	Dependencia: Oficina Asesora de Planeación y Desarrollo.