DNDA
Dirección Nacional de Derecho de Autor
Ministerio del Interior

Política de administración de riesgos
Dirección Nacional de Derecho de Autor

2022

El futuro es de todos
Mininterior

POLÍTICA DE ADMINISTRACIÓN DE RIESGOS
DIRECCIÓN NACIONAL DE DERECHO DE AUTOR

1. OBJETIVO DE LA POLÍTICA DE RIESGOS

Establecer los lineamientos para la administración y control de los riesgos de gestión, seguridad de la información y corrupción en la Unidad Administrativa Especial Dirección Nacional de Derecho de Autor (DNDA), para una adecuada identificación, medición, control y monitoreo; y así mismo, minimizar la probabilidad de su materialización para evitar afectación sobre el cumplimiento de las metas institucionales y gestionarlos a un nivel aceptable.

2. ALCANCE

Este documento aplica para todos los procesos de la Entidad (estratégicos, misionales y de apoyo), y para todas las acciones ejecutadas por los servidores durante el ejercicio de sus funciones.

3. ANTECEDENTES

La Dirección Nacional del Derecho de Autor se crea como una Unidad Administrativa Especial, con personería jurídica, autonomía administrativa y patrimonio independiente, adscrita al Ministerio de Gobierno, hoy Ministerio del Interior, mediante el Decreto 2041 del 29 de agosto de 1991.

Sobre su jurisdicción, competencia y domicilio: Sus competencias en dicho decreto fueron el diseño, dirección, administración y ejecución de las políticas gubernamentales en materia de derechos de autor; llevar el registro nacional de las obras literarias y artísticas y ejercer la inspección y vigilancia sobre las sociedades de gestión colectiva de los derechos reconocidos en la Ley 23 de 1982 y demás disposiciones. El ámbito de las funciones de la Dirección Nacional del Derecho de Autor comprende todo el territorio nacional, teniendo su domicilio principal en la ciudad de Bogotá.

Sobre su patrimonio: El patrimonio de la DNDA está constituido por:

- a) Las partidas ordinarias y extraordinarias asignadas en el Presupuesto Nacional y los recursos propios.
- b) Las donaciones nacionales e internacionales que reciba.
- c) Los bienes muebles e inmuebles que adquiera o haya adquirido a cualquier título.
- d) Los rendimientos financieros obtenidos de sus recursos propios.
- e) Los recursos provenientes del crédito externo e interno.
- f) Los demás que obtenga a cualquier título.

Sobre su Control Fiscal: La vigilancia de la gestión fiscal de la DNDA es ejercida por la Contraloría General de la República.

Sobre su Representante Legal: El director general de esta entidad es su representante legal, cuyo nombramiento es efectuado por el Presidente de la República o por el Ministro de Interior si se ha delegado en él esta competencia.

Sobre su Régimen Jurídico: El régimen jurídico aplicable en materia presupuestal, de administración de personal y de contratación será el mismo que rige para los establecimientos públicos, ajustado a la naturaleza jurídica y a la estructura que determina este Decreto.

Sobre sus objetivos y funciones:
Objetivo Institucional de la DNDA

Contribuir a los fines esenciales del Estado colombiano, mediante el diseño, dirección, administración y ejecución de las políticas gubernamentales en materia de derecho de autor y derechos conexos, asegurando la protección de los derechos de los autores y titulares de las obras literarias y artísticas, contribuyendo a la creación de una cultura de respeto por dichos derechos y fomentando un ambiente propicio para la creación y difusión de nuevas obras como expresión del desarrollo económico, artístico y cultural del país.

Funciones:

El Decreto 2041 de 1991, le asigna a la Dirección Nacional de Derecho de Autor los siguientes cometidos institucionales:

1. Diseñar, administrar y ejecutar las políticas gubernamentales en materia de derecho de autor y derechos conexos.
2. Administrar el registro nacional de las obras literarias, artísticas, y de los actos o contratos vinculados con el derecho de autor o los derechos conexos.
3. Ejercer la facultad de inspección y vigilancia sobre las sociedades de gestión colectiva de derecho de autor y derechos conexos.
4. Recomendar la adhesión y procurar la ratificación y aplicación a los tratados internacionales sobre derecho de autor y derechos conexos.

5. Dictar las providencias necesarias con el objeto de cumplir los acuerdos internacionales sobre derecho de autor y derechos conexos.
6. Capacitar y difundir el conocimiento del derecho de autor y los derechos conexos.

4. TÉRMINOS Y DEFINICIONES

A continuación, se relacionan los conceptos básicos y necesarios para la comprensión de la metodología que se desarrollará a través del presente documento.

- **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. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.

- **Activo:** en el contexto de seguridad digital o de la información, 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.

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

- **Cadena de valor:** la interrelación de los procesos dirigidos a satisfacer las necesidades y requisitos de los usuarios (procesos misionales).

- **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.

- **Caracterización de proceso:** estructura que permite identificar los rasgos distintivos de los procesos. Establece su objetivo, la relación con los demás procesos, los insumos, los activos, su transformación a través de las actividades que desarrolla y las salidas del proceso, se identifican los proveedores y clientes o usuarios, que pueden ser internos o externos.

- **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 la 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 ser accesible y utilizable a demanda por una entidad.

- **Factores de riesgo:** son las fuentes generadoras de riesgos.

- **Impacto:** las consecuencias que puede ocasionar a la organización la materialización del riesgo.

- **Integridad:** propiedad de exactitud y completitud.

- **Mapa de riesgos:** documento con la información resultante de la gestión del riesgo.

- **Mapa de procesos:** es la representación gráfica de los procesos estratégicos, misionales, de apoyo, de evaluación y sus interacciones. Constituye la razón de ser de la entidad, sintetiza los principales propósitos estratégicos y los valores esenciales que deben ser conocidos, comprendidos y compartidos por todas las personas que hacen parte de la entidad.

- **Modelo de operación por procesos:** el modelo de operación por procesos es el estándar organizacional que soporta la operación de la entidad pública, integrando las competencias constitucionales y legales que la rigen con el conjunto de planes y programas necesarios para el cumplimiento de su misión, visión y objetivos institucionales. Pretende determinar la mejor y más eficiente forma de ejecutar las operaciones de la entidad.

- **Objetivo del proceso:** es el resultado que se espera lograr para cumplir la misión y visión; determina el cómo logro la política trazada y el aporte que se hace a los objetivos institucionales. Un objetivo es un enunciado que expresa una acción, por lo tanto, debe iniciarse con un verbo fuerte como: establecer, identificar, recopilar, investigar, registrar, buscar. Los objetivos deben ser: medibles, realistas y se deben evitar frases subjetivas en su construcción.

- **Objetivos estratégicos:** Identifican la finalidad hacia la cual deben dirigirse los recursos y

esfuerzos para dar cumplimiento al mandato legal aplicable a cada entidad; estos objetivos institucionales se materializan a través de la ejecución de la planeación anual de cada entidad.

- **Plan anticorrupción y de atención al ciudadano:** contempla la estrategia de lucha contra la corrupción que debe ser implementada por todas las entidades del orden nacional, departamental y municipal.

- **Planeación institucional:** las estrategias de la entidad generalmente se definen por parte de la alta dirección y obedecen a la razón de ser que desarrolla la misma, a los planes sectoriales, las políticas específicas que define el Gobierno nacional, departamental o municipal enmarcadas dentro del Plan Nacional de Desarrollo. En este contexto la entidad define su planeación institucional. La planeación institucional hace uso de los procesos estratégicos, misionales, de apoyo y evaluación para materializarla o ejecutarla; por lo tanto, la administración del riesgo no puede verse de forma aislada.

- **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.

- **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.

- **Riesgo:** efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales. Los eventos potenciales hacen referencia a la posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos.

- **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.

► **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.

5. ROLES Y RESPONSABILIDADES

El diseño y actualización del presente documento, está a cargo de la Oficina Asesora de Planeación, y la aprobación de este, se llevará a cabo por parte del Comité Institucional de Coordinación de Control Interno.

Por otro lado, la Unidad Administrativa Especial Dirección Nacional de Derecho de Autor, determina las siguientes responsabilidades en relación con las líneas de defensa establecidas en el Modelo Integrado de Planeación y Gestión – MIPG, así:

LÍNEA ESTRATÉGICA	
Define el marco general para la gestión del riesgo y el control (política de administración del riesgo) y supervisa su cumplimiento.	
RESPONSABLES	
Alta Dirección Comité Institucional de Coordinación de Control Interno	
1ª. LÍNEA DE DEFENSA	
Desarrolla e implementa procesos de control y gestión de riesgos a través de su identificación, valoración, monitoreo y acciones de mejora.	
RESPONSABLES	**ROLP RINCIPAL**
Subdirectores y asesores	Diseñar, implementar y monitorear los controles y gestionar de manera directa en el día a día los riesgos de la entidad. Le corresponde a los líderes de proceso asegurar la implementación de esta metodología para mitigar los riesgos en la operación, reportando a la Oficina Asesora de Planeación sus avances y dificultades; esto incluye comunicar la actualización de riesgos identificados cada vez que se presente. Los servidores son los responsables de ejecutar controles operativos en el día a día.

2ª. 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 funciones como se pretende.

RESPONSABLES	ROL PRINCIPAL
Oficina Asesora de Planeación, Supervisores de contratos o proyectos	Monitorear la gestión de riesgo y control ejecutada por la primera línea de defensa, complementando su trabajo. Le corresponde a la Oficina Asesora de Planeación definir la metodología, capacitar y acompañar con el fin de asegurar la implementación de los lineamientos definidos. A la vez, está a cargo de esta oficina la socialización del mapa de riesgos de la entidad a sus partes interesadas, incluyendo cada modificación que se realice sobre el mismo.

3ª. LÍNEA DE DEFENSA

Proporciona información sobre la efectividad del Sistema de Control Interno, a través de un enfoque basado en riesgos, incluida la operación de la primera y segunda línea de defensa.

RESPONSABLES	ROL PRINCIPAL
Oficina de Control Interno	Proporcionar un aseguramiento a través de la auditoría interna; por lo tanto, debe dar a conocer a toda la entidad el Plan Anual de Auditorías basado en riesgos, y los resultados de la evaluación de la gestión del riesgo. De igual manera, asesora de forma coordinada con la Oficina de Planeación, a la primera línea de defensa en la identificación de los riesgos institucionales y diseño de controles.

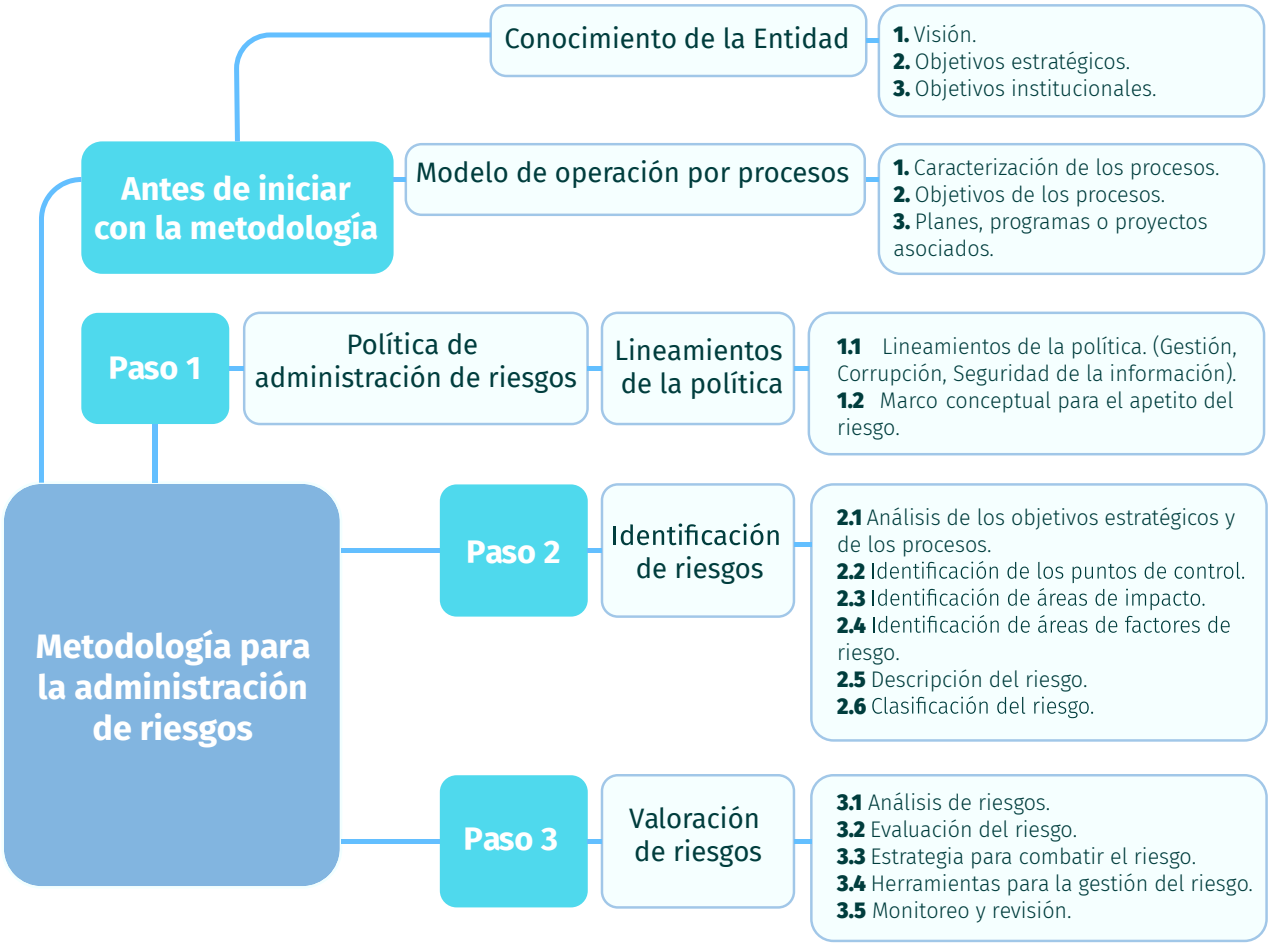
6. METODOLOGÍA

La Dirección Nacional de Derecho de Autor aplicará la metodología establecida por el Departamento Administrativo de la Función Pública, descrita en la Guía para la administración de riesgos y el diseño de controles en entidades públicas, Versión 5.

Antes de dar inicio a la metodología para la administración del riesgo, es importante tener conocimiento de la entidad respecto a su contexto estratégico (misión, visión, objetivos institucionales y planeación institucional); por otra parte, es esencial operar por procesos, con el fin de contemplar la información asociada a los mismos (caracterización y objetivo del proceso, planes, programas o proyectos).

Esta metodología, se desarrolla a través de tres (3) pasos básicos:

- **Paso 1.** Política de administración del riesgo
- **Paso 2.** Identificación de riesgos
- **Paso 3.** Valoración de riesgos



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

PASO 1. POLÍTICA DE ADMINISTRACIÓN DEL RIESGO

La alta Dirección de la Dirección Nacional de Derecho de Autor se compromete a administrar adecuadamente los riesgos a los que se encuentra expuesta y que pueden interferir en el logro de la misión, los objetivos institucionales y su imagen ante grupos de valor y de interés; lo anterior, atendiendo los lineamientos definidos a través de la metodología establecida para su identificación, valoración, control y monitoreo; determinando a su vez, las acciones necesarias de control preventivas de manera oportuna, para evitar su materialización y así mismo, mitigar las posibles consecuencias a fin de mantener los niveles de riesgo aceptables.

PASO 2. IDENTIFICACIÓN DEL RIESGO

- A través de este paso se deben identificar los riesgos que estén o no bajo el control de la entidad y para lo cual se debe tener en cuenta lo siguiente:

- Analizar los objetivos estratégicos para identificar posibles riesgos que afectan su cumplimiento.

- Analizar el objetivo y alcance del respectivo proceso (caracterización), verificando que se encuentre alineado con la misión y visión de la entidad, para asegurar que contribuya a los objetivos estratégicos.

- Identificar áreas de impacto: es la consecuencia económica o reputacional a la cual se ve expuesta la entidad en caso de materializarse un riesgo. Los impactos que aplican son afectación económica (o presupuestal) y reputacional.

Identificación del riesgo

FACTOR	DEFINICIÓN	DESCRIPCIÓN
PROCESOS	Eventos relacionados con errores en las actividades que deben realizar los servidores de la organización.	- Falta de procedimientos. - Errores de grabación, autorización. - Errores en cálculos para pagos internos y externos. Falta de capacitación, temas relacionados con el personal

FACTOR	DEFINICIÓN	DESCRIPCIÓN
TALENTO HUMANO	Incluye seguridad y salud en el trabajo. Se analiza posible dolo e intención frente a la corrupción.	- Hurto de activos. - Posibles comportamientos no éticos de los empleados. - Fraude interno (corrupción, soborno). - Falta de capacitación, temas relacionados con el personal.
TECNOLOGÍA	Eventos relacionados con la infraestructura tecnológica de la entidad.	- Daño de equipos. - Caída de aplicaciones. - Caída de redes. - Errores en programas.
INFRAESTRUCTURA	Eventos relacionados con la infraestructura física de la entidad.	- Derrumbes. - Incendios. - Inundaciones. - Daños a activos fijos.
EVENTO EXTERNO	Situaciones externas que afectan la entidad.	- Suplantación de identidad. - Asalto a la oficina. - Atentados, vandalismo, orden público.

Determine las causas por las cuales se puede generar el riesgo. Los tipos de causa corresponden a:

- **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 puede existir más de una causa o subcausas que pueden ser analizadas.

EJEMPLO	
CAUSA INMEDIATA ¿Cómo?	**CAUSA RAÍZ ¿Por qué?**
Multa y sanción del organismo de control	- Adquisición de bienes y servicios fuera de los requerimientos normativos. - Incumplimiento de los requisitos para contratación.

Clasificación del riesgo

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

CLASIFICACIÓN		FACTORES DE RIESGO
EJECUCIÓN Y ADMINISTRACIÓN DE PROCESOS	Pérdidas derivadas de errores en la ejecución y administración de procesos.	PROCESOS
FRAUDE EXTERNO	Pérdida derivada de actos de fraude por personas ajenas a la organización (no participa personal de la entidad).	EVENTO EXTERNO
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.	TALENTO HUMANO
FALLAS TECNOLÓGICAS	Errores en hardware, software, telecomunicaciones, interrupción de servicios básicos.	TECNOLOGÍA
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.	PUEDEN ASOCIARSE A VARIOS FACTORES
USUARIOS, PRODUCTOS Y PRÁCTICAS	Fallas negligentes o involuntarias de las obligaciones frente a los usuarios y que impiden satisfacer una obligación profesional frente a éstos.	
DAÑOS A ACTIVOS FIJOS/EXTERNOS	Pérdida por daños o extravíos de los activos fijos por desastres naturales u otros riesgos/eventos externos como atentados, vandalismo, orden público.	INFRAESTRUCTURA EVENTO EXTERNO

De acuerdo con la naturaleza de la entidad, los objetivos institucionales y el ciclo de operación, se indican los tipos de riesgo que serán administrados y controlados por la Unidad:

- **Gestión**
- **Corrupción**
- **Seguridad de la información**

Descripción del riesgo

Para la redacción de los riesgos de gestión, corrupción y seguridad de la información, se adoptan los esquemas propuestos por el Departamento Administrativo de la Función Pública, a través de la guía para la administración del riesgo y el diseño de controles en entidades públicas, así:

RIESGOS DE GESTIÓN

Redacción inicia con:	¿Qué?	¿Cómo?	¿Por qué?
Posibilidad de:	Afectación económica Impacto	Por multa y sanción del ente regulador Causa Inmediata	Debido a adquisición de bienes y servicios fuera de los requerimientos normativos. Causa Raíz

Ejemplo: Posibilidad de afectación económica por multa y sanción del organismo de control, debido la adquisición de bienes y servicios fuera de los requerimientos normativos.

TENGA EN CUENTA	EJEMPLO
X No describir como riesgos, omisiones ni desviaciones del control.	Errores en la liquidación de la nómina por fallas en los procedimientos existentes.
X No describir causas como riesgos.	Inadecuado funcionamiento de la plataforma estratégica donde se realiza el seguimiento a la planeación.
X No describir riesgos como la negación de un control.	Retrasos en la prestación del servicio por no contar con digiturno para la atención.
X No existen riesgos transversales, lo que pueden existir son causas transversales.	Pérdida de expedientes.

RIESGOS DE CORRUPCIÓN

Es necesario que, en la descripción del riesgo concurran los componentes de su definición así:

ACCIÓN U OMISIÓN + **USO DEL PODER** + **DESVIACIÓN DE LA GESTIÓN DE LO PÚBLICO** + **EL BENEFICIO PRIVADO**

Propio o de terceros con el fin celebrar un contrato.

RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Estos riesgos se basan en la afectación de tres criterios en un activo, y por lo tanto su redacción corresponderá a:

Ejemplo:

- **Pérdida de integridad**
- **Pérdida de disponibilidad**
- **Pérdida de confidencialidad**

Identifique los activos de información (solo aplican para riesgos de seguridad de la información).

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

De igual manera, permite determinar qué es lo más importante que cada entidad y sus procesos poseen (sean bases de datos, archivos, servidores web o aplicaciones clave para que la entidad pueda prestar sus servicios).

Los pasos a seguir para identificar los activos de información corresponden a:

Paso 1	Paso 2	Paso 3	Paso 4	Paso 5	Paso 6
Listar los activos por cada proceso	**Identificar el dueño de los activos**	**Clasificar los activos**	**Clasificar la información**	**Determinar la criticidad del activo**	**Identificar si existe infraestructura crítica cibernética**

La identificación y valoración de activos debe ser realizada por la 1ª Línea de defensa – líderes de proceso, en cada proceso donde aplique la gestión del riesgo de seguridad de la información, con la orientación del responsable de seguridad digital o de seguridad de la información de la entidad pública; en este caso por el CIO (Chief Infgormation Officer) de la DNDA.

Para profundizar sobre esta identificación, el Departamento Administrativo de la Función Pública sugiere remitirse a la sección 3.1.6 del "Modelo nacional de gestión de riesgo de seguridad de la información en entidades públicas" del Ministerio de Tecnologías de la Información y las Comunicaciones, el cual hace parte integral de la presente guía.

PASO 3. VALORACIÓN DEL RIESGO

La valoración permite establecer la probabilidad de ocurrencia del riesgo y el nivel de impacto, con el fin de estimar la zona de riesgo inicial (RIESGO INHERENTE), y a través de la evaluación del riesgo se busca confrontar los resultados del análisis del riesgo inicial, frente a los controles establecidos, con el fin de determinar la zona de riesgo final (RIESGO RESIDUAL).

PROBABILIDAD:

A través de la siguiente tabla, se establecen los criterios para definir el nivel de probabilidad para los riesgos de **GESTIÓN, CORRUPCIÓN Y SEGURIDAD DE LA INFORMACIÓN.**

	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.	**20%**
Media	La actividad que conlleva el riesgo se ejecuta de 25 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 mas de 5000.	**100%**

IMPACTO

A través de la siguiente tabla, se establecen los criterios para definir el nivel de impacto para riesgos de **GESTIÓN y SEGURIDAD DE LA INFORMACIÓN.**

Afectación Económica		Reputacional
Leve 20%	Afectación menor a 10 SMLMV	El riesgo afecta la imagen de algún área de la organización.
Menor -40%	Entre 50 y 100 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 -60%	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	Mayor a 500 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país.

Por otra parte, la siguiente tabla indica los criterios para calificar el impacto en riesgos de **CORRUPCIÓN.**

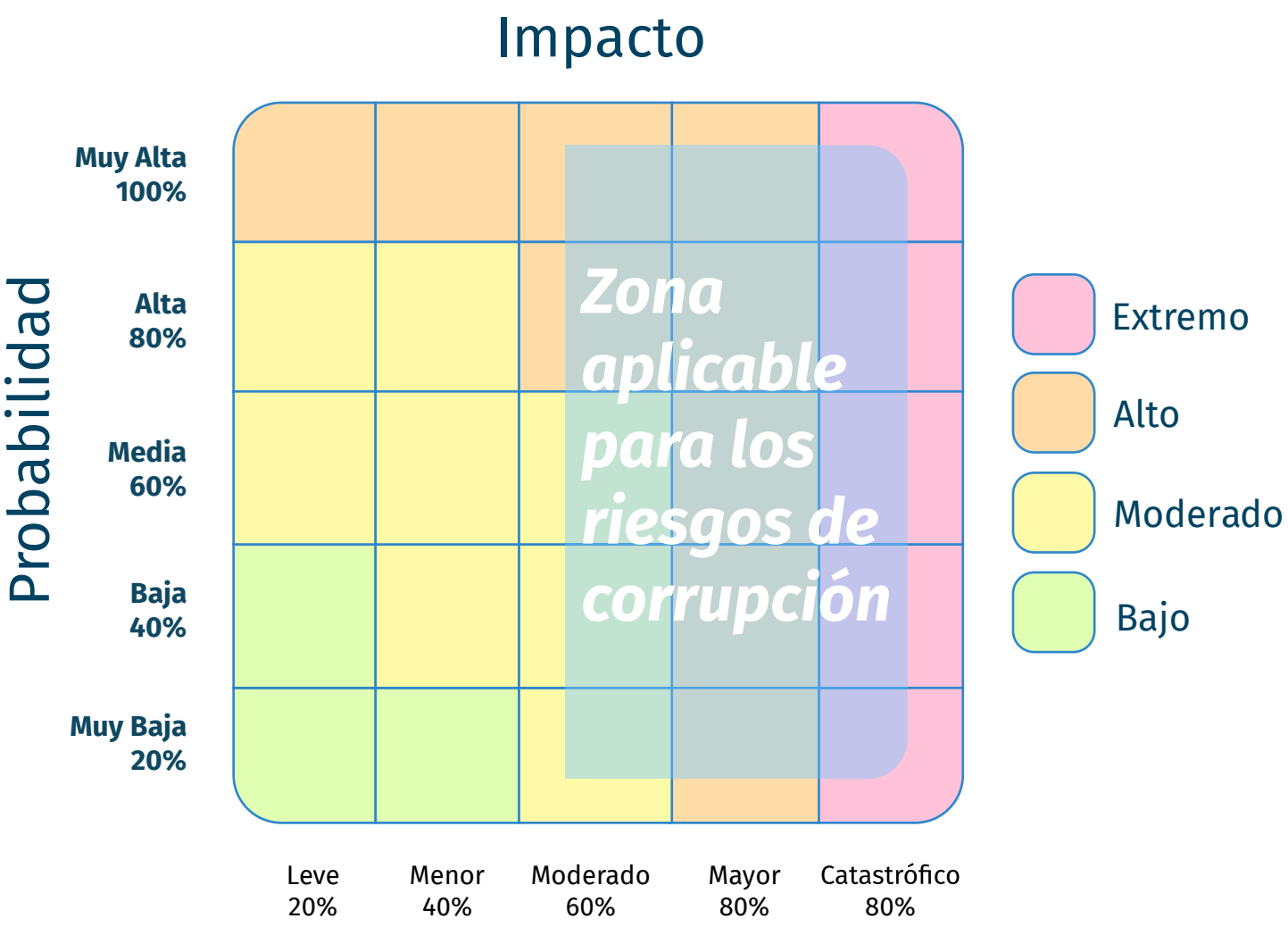
N.	Pregunta: Si el riesgo de corrupción se materializa podría...	Respuesta SI	Respuesta NO
1.	¿Afectar al grupo de funcionarios del estado?	X	
2.	¿Afectar el cumplimiento de metas y objetivos de la dependencia?	X	
3.	¿Afectar el cumplimiento de misión de la entidad?	X	
4.	¿Afectar el cumplimiento de la misión del sector al que pertenece la entidad?		X
5.	¿Generar perdida de confianza de la entidad, afectando su reputación?	X	

6.	¿Generar pérdida de recursos económicos?	X	
7.	¿Afectar la generación de los productos o la prestación de servicios?	X	
8.	¿Dar lugar al detrimento de calidad de vida de la comunidad por la perdida del bien, servicios o recursos públicos?		X
9.	¿Genera pérdida de información de la entidad?		X
10.	¿Generar intervención de los órganos de control, de la Fiscalía u otro ente?	X	
11.	¿Dar lugar a procesos sancionatorios?	X	
12.	¿Dar lugar a procesos disciplinarios?	X	
13.	¿Dar lugar a procesos fiscales?	X	
14.	¿Dar lugar a procesos penales?		X
15.	¿Generar pérdida de credibilidad del sector?		X
16.	¿Ocasionar lesiones físicas o pérdida de vidas humanas?		X
17.	¿Afectar la imagen regional?		X
18.	¿Afectar la imagen nacional?		X
19.	¿Generar daño ambiental?		X
Responder afirmativamente de UNA a CINCO preguntas(s) genera un impacto moderado. Responder afirmativamente de SEIS a ONCE preguntas genera un impacto mayor. Responder afirmativa de DOCE a DIECINUEVE preguntas genera un impacto catastrófico.		10	
Moderado	Moderado Genera medianas consecuencias sobre la entidad.		
Mayor	Mayor: Genera altas consecuencias sobre la entidad.		
Catastrófico	Catastrófico: Genera consecuencias desastrosas para la entidad.		

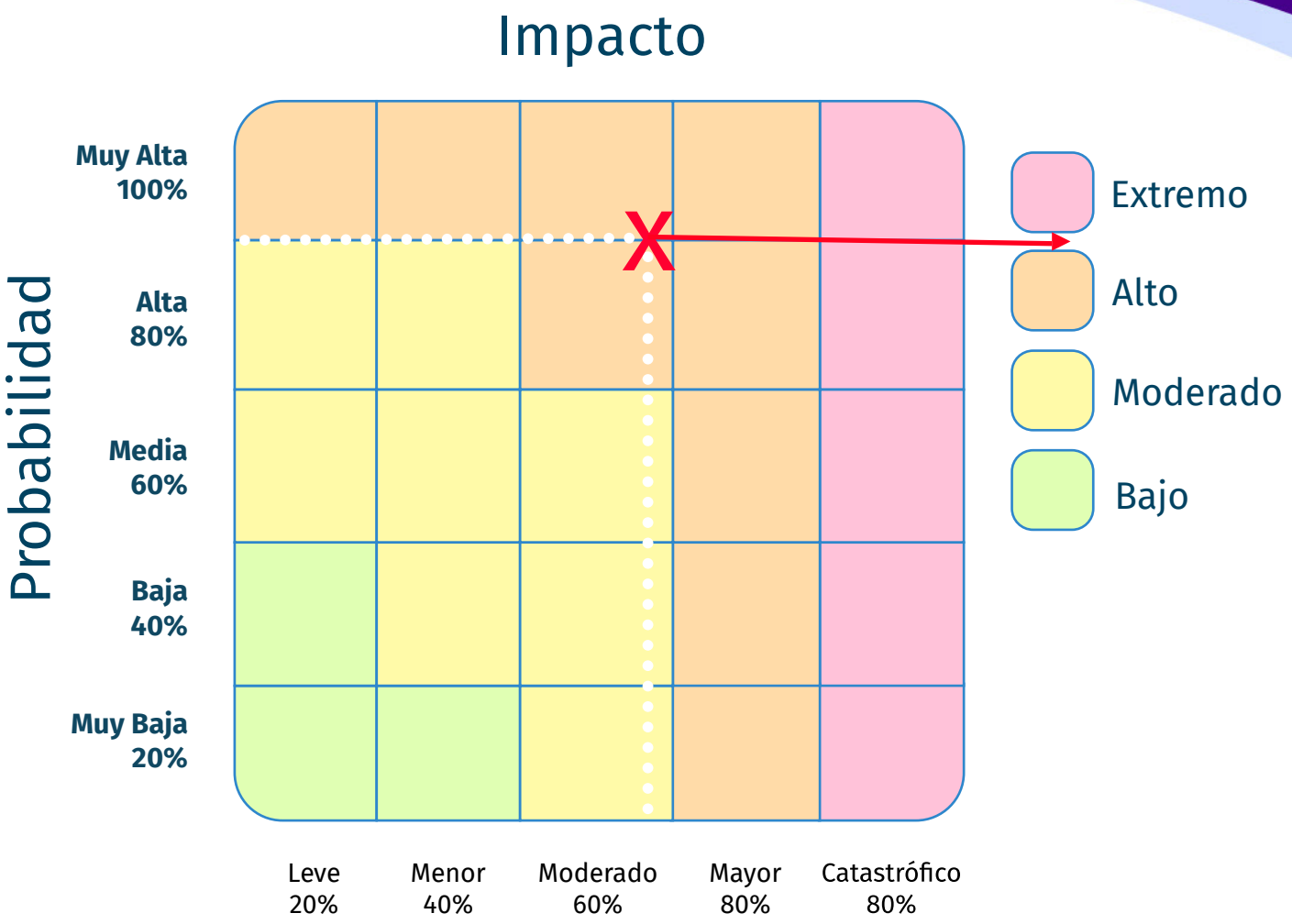
Nivel de impacto MAYOR

ZONA DE RIESGO – MAPA DE CALOR

Se trata de determinar los niveles de severidad a través de la combinación entre la probabilidad y el impacto. Se definen cuatro (4) zonas de severidad en la matriz de calor **(BAJO, MODERADO, ALTO, EXTREMO).** A través de esta tabla se define la zona de riesgo inherente y zona de riesgo residual:



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 los riesgos de gestión y de seguridad de la información.



Es importante recordar que, el riesgo inherente es aquel con el cual se enfrenta la entidad antes de implementar controles, y el riesgo residual, es aquel que permanece a pesar de haberlos implementado.

EVALUACIÓN DEL RIESGO – VALORACIÓN DE CONTROLES

► **Descripción de controles**

Para una adecuada redacción del control, se debe tener en cuenta la siguiente estructura.

- **Responsable de ejecutar el control: I**dentifica 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.

Ejemplo:

Responsable	El profesional de Contratación.
Acción	Verifica que la información suministrada por el proveedor corresponda con los requisitos establecidos acorde con el tipo de contratación.
Complemento	A través de una lista de chequeo donde están los requisitos de información y la revisa con la información física suministrada por el proveedor, los contratos que cumplen son registrados en el sistema de información de contratación.

De acuerdo a lo anterior, a continuación se presentan los atributos asociados a los controles que serán identificados a través del mapa de riesgos de gestión, seguridad de la información y corrupción de la entidad:

CARACTERÍSTICAS			DESCRIPCIÓN
ATRIBUTOS DE EFICIENCIA	**Tipo**	**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.
		Detectivo	Detecta que algo ocurre y devuelve el proceso a los controles preventivos. Se pueden generar reprocesos.
		Correctivo	Dado que permiten reducir el impacto de la materialización del riesgo, tienen un costo en su implementación.
	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.
		Manual	Controles que son ejecutados por una persona, tiene implícito el error humano.

CARACTERÍSTICAS			DESCRIPCIÓN
ATRIBUTOS DE FORMALIZACIÓN	**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.
	Evidencia	**Con registro**	El control deja un registro que permite evidenciar la ejecución del control.
		Sin registro	El control no deja registro de la ejecución del control.

TRATAMIENTO DEL RIESGO

Decisión que se toma frente a un determinado nivel de riesgo, dicha decisión puede ser aceptar, reducir o evitar y se analiza frente al riesgo residual.

REDUCIR **ALTO** **MODERADO**	Después de realizar un análisis, y considerar que el nivel de riesgo es ALTO o MODERADO, se determina tratarlo mediante:	**1. Compartir:** después de realizar un análisis, se considera que la mejor estrategia es tercerizar el proceso o trasladar el proceso a través de seguros o pólizas. La responsabilidad económica recae sobre el tercero, pero no se transfiere la responsabilidad sobre el tema reputacional.	Generar plan de acción bajo la medida de mitigar el riesgo.
		2. Mitigar: después de realizar un análisis y considerar los niveles de riesgo, se implementan acciones que mitiguen el nivel del riesgo (plan de acción). No necesariamente es un control adicional.	

ACEPTAR **BAJO**	Después de realizar un análisis y considerar los niveles de riesgo, se determina asumir el mismo, conociendo los efectos de su posible materialización. En este caso, se acepta el riesgo y se administra por medio de las actividades propias del proceso asociado y su control. Los riesgos de corrupción nunca se podrán aceptar.	En este caso, no es necesario indicar plan de acción.
EVITAR **EXTREMO**	Después de realizar un análisis y considerar que el nivel de riesgo es EXTREMO, se determina NO asumir la actividad que genera este riesgo.	

MONITOREO Y REVISIÓN

- La identificación de riesgos de gestión, corrupción y seguridad de la información, es un ejercicio que se debe desarrollar de manera anual por cada responsable de proceso, junto con su equipo de trabajo.

- La consolidación del mapa de riesgos institucional se lleva a cabo a través de la Oficina Asesora de Planeación. Para tal fin, la entidad cuenta con una estructura independiente para riesgos de gestión y de seguridad de la información, y una estructura para riesgos de corrupción.

- La aprobación del mapa de riesgos institucional la realiza el Comité Institucional de Gestión y Desempeño con previa aprobación de cada uno de los líderes de los procesos.

- Después de su publicación y durante el respectivo año de vigencia, se podrán realizar los ajustes y las modificaciones necesarias orientadas a mejorar el mapa de riesgos. En este caso, deberán relacionarse en el historial de cambios del mapa los ajustes, modificaciones o inclusiones realizadas.

De acuerdo con la cultura del autocontrol al interior de la entidad, los líderes de los procesos junto con su equipo de trabajo, realizarán monitoreo y evaluación de manera permanente, con el fin de analizar el estado de sus procesos frente a los controles establecidos. Los resultados de este monitoreo, se evidenciarán a través de su socialización en las sesiones de comité directivo que desarrolla la entidad.

La Oficina de Control Interno, debe adelantar seguimiento a la gestión de los riesgos institucionales. En este sentido, es necesario que en sus procesos de auditoría interna se analicen las causas, los riesgos, la efectividad de los controles incorporados en el mapa de riesgos institucional y el cumplimiento de las acciones planteadas.

HISTORIAL DE CAMBIOS

VERSIÓN	OBSERVACIONES	FECHA
1	Se crea el documento	julio de 2022

Síguenos en:

@derechodeautor

@derechodeautor

derechodeautorcol

@derechodeautor

/company/derechodeautor

www.derechodeautor.gov.co

@Derechodeautorcol

Contáctanos:

Teléfono: 6017868220
Línea PQRSF: 01 8000 127878
info@derechodeautor.gov.co
Calle 28 Nº 13 A - 15 Piso 17. Bogotá D.C, Colombia

Política de administración de riesgos
Dirección Nacional de Derecho de Autor

2022

El futuro es de todos

Mininterior

DNDA
Dirección Nacional de Derecho de Autor
Ministerio del Interior