

POLÍTICA DE ADMINISTRACIÓN DEL RIESGO

INSTITUTO NACIONAL PARA CIEGOS

Versión 3

Agosto de 2021

BOGOTÁ, D.C.

Contenido

[Introducción 3](#_Toc79578465)

[Objetivo 3](#_Toc79578466)

[Alcance 3](#_Toc79578467)

[METODOLOGÍA PARA LA ADMINISTRACIÓN DEL RIESGO 4](#_Toc79578468)

[**1.** **ESTABLECIMIENTO DEL CONTEXTO:** 4](#_Toc79578469)

[1.1. Contexto Externo: 5](#_Toc79578470)

[1.2. Contexto Interno: 5](#_Toc79578471)

[1.3. Contexto del proceso: 6](#_Toc79578472)

[**2.** **IDENTIFICACIÓN DE RIESGOS:** 7](#_Toc79578473)

[2.1. Análisis de objetivos estratégicos y de procesos: 7](#_Toc79578474)

[2.2. Tipos de Riesgo 8](#_Toc79578475)

[2.3. Identificación de los puntos de riesgo: 9](#_Toc79578476)

[2.4. Identificación de áreas de impacto: 9](#_Toc79578477)

[2.5. Identificación de áreas de factores de riesgo: 9](#_Toc79578478)

[2.6. Descripción del riesgo: 10](#_Toc79578479)

[2.7. Clasificación del riesgo: 12](#_Toc79578480)

[**3.** **Valoración del riesgo** 13](#_Toc79578481)

[3.1. Análisis de riesgos: 13](#_Toc79578482)

[3.2. Evaluación de riesgos: 15](#_Toc79578483)

[3.3. Estrategias para combatir el riesgo: 22](#_Toc79578484)

[3.4. Monitoreo y revisión: 23](#_Toc79578485)

[**4.** **LINEAMIENTOS SOBRE RIESGOS RELACIONADOS CON POSIBLES ACTOS DE CORRUPCIÓN** 27](#_Toc79578486)

[4.1. Identificación del riesgo de corrupción 28](#_Toc79578487)

[**4.2.** **Valoración del riesgo** 29](#_Toc79578488)

[**5.** **LINEAMIENTOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN** 32](#_Toc79578489)

[5.1. Identificación de los activos de seguridad de la información: 32](#_Toc79578490)

[5.2. Identificación del riesgo: 33](#_Toc79578491)

[5.3. Valoración del riesgo: 34](#_Toc79578492)

[5.4. Controles asociados a la seguridad de la información 34](#_Toc79578493)

[**6.** **NIVELES DE ACEPTACIÓN DEL RIESGO:** 36](#_Toc79578494)

[**7.** **ACCIONAR ANTE LOS RIESGOS MATERIALIZADOS** 37](#_Toc79578495)

[Referencias 38](#_Toc79578496)

# Introducción

El Instituto Nacional para Ciegos, estructura el presente documento tomando como referente los parámetros del Modelo Integrado de Planeación y Gestión y los lineamientos de la Guía para la administración del riesgo y el diseño de controles en entidades públicas del Departamento Administrativo de la Función Pública de Diciembre de 2020[[1]](#footnote-1), la cual contempla los riesgos de gestión, corrupción y de seguridad digital.

Esta política establece los lineamientos que permitan la identificación, el análisis, la valoración, tratamiento y monitoreo de los riesgos que pudieran afectar la misión y el cumplimiento de los objetivos institucionales en el marco de los proyectos, planes y procesos del INCI a través de:

* La identificación y documentación de riesgos de gestión, corrupción y seguridad digital.
* El establecimiento de controles y acciones preventivas para los riesgos identificados
* La actuación correctiva y oportuna ante la materialización de los riesgos identificados.

# Objetivo

Establecer el marco general de actuación para la gestión de los riesgos a los que puede enfrentarse el Instituto Nacional para Ciegos en el desarrollo de sus acciones, a través de los lineamientos establecidos para la identificación, análisis, evaluación, tratamiento y monitoreo de los riesgos que puedan afectar la gestión y el cumplimiento de los objetivos de la institución.

# Alcance

La política de administración de riesgos es aplicable a todos los procesos de la Entidad y a las acciones ejecutadas por los servidores durante el ejercicio de sus funciones.

Antes de iniciar con la metodología es necesario tener claro que la identificación y valoración de riesgos debe estar articulada con los objetivos de la entidad y de los diferentes procesos así como con la implementación de esos objetivos que apuntan al cumplimiento de la misión institucional.

# METODOLOGÍA PARA LA ADMINISTRACIÓN DEL RIESGO

## **ESTABLECIMIENTO DEL CONTEXTO:**

Para realizar la identificación de los riesgos que puedan afectar el cumplimiento de los objetivos institucionales, se debe iniciar analizando el contexto de cada uno de los procesos del Sistema Integrado de Gestión. Para ello, debe analizar el contexto interno, externo y el del mismo proceso, ya que a partir de los factores que se definan es posible establecer las causas de los riesgos a identificar.

Para ello, debe diligenciar la matriz DOFA que se encuentra en la hoja Número 1 denominada Análisis de Contexto del formato “Mapa de Riesgos Institucional” la cual contiene la siguiente información:

Nombre del proceso

Objetivo del proceso:

Fecha de elaboración:

Tabla No 1 Análisis del contexto y estrategias DOFA

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| CONTEXTO EXTERNO | OPORTUNIDAD | AMENAZA |  | Estrategias DO | Estrategias FA | Estrategias FO |
| Político |  |  |  |  |  |  |
| Económico y financiero |  |  |  |  |  |  |
| Social Cultural |  |  |  |  |  |  |
| Tecnológico |  |  |  |  |  |  |
| Ambiental |  |  |  |  |  |  |
| Legal y Reglamentario |  |  |  |  |  |  |
| CONTEXTO INTERNO | DEBILIDAD | FORTALEZA |  |  |  |  |
| Financiero |  |  |  |  |  |  |
| Personal |  |  |  |  |  |  |
| Procesos |  |  |  |  |  |  |
| Tecnología |  |  |  |  |  |  |
| Estratégico |  |  |  |  |  |  |
| Comunicación Interna |  |  |  |  |  |  |
| CONTEXTO DEL PROCESO | DEBILIDAD | FORTALEZA |  |  |  |  |
| Diseño del Proceso |  |  |  |  |  |  |
| Interacción con otros procesos |  |  |  |  |  |  |
| Transversalidad |  |  |  |  |  |  |
| Procedimientos Asociados |  |  |  |  |  |  |
| Responsables del Proceso |  |  |  |  |  |  |
| Comunicación Entre Procesos |  |  |  |  |  |  |
| Activos de Seguridad Digital del Proceso |  |  |  |  |  |  |

### Contexto Externo:

Se determinan las características o aspectos esenciales del entorno en el cual opera la entidad. Se pueden considerar los siguientes:

* Factores políticos: cambios de gobierno, legislación y políticas públicas.
* Económicos y financieros: disponibilidad de recursos.
* Sociales y Culturales: demografía, responsabilidad social, orden público
* Tecnológicos: avances en tecnología, acceso a sistemas de información externos, gobierno digital
* Ambientales: emisiones y residuos, energía, catástrofes naturales
* Legales y reglamentarios: leyes, decretos, ordenanzas y acuerdos

### Contexto Interno:

Se determinan las características o aspectos esenciales del ambiente en el cual la entidad busca alcanzar sus objetivos. Se pueden considerar los siguientes factores:

* Financieros: presupuesto de funcionamiento y recursos de inversión.
* Personal: competencia y 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.

### 1.3. Contexto del proceso:

Se determinan las características o aspectos esenciales del proceso y sus interrelaciones. Se pueden considerar los siguientes factores:

* 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.

## **IDENTIFICACIÓN DE RIESGOS:**

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.

### Análisis de objetivos estratégicos y de procesos:

Todos los riesgos que se identifiquen deben tener impacto en el cumplimiento de los objetivos estratégicos o de proceso y a su vez estos deben estar alineados con la Misión y la Visión de la Entidad. Dichos objetivos deben ser medibles, alcanzables y deben incluir el que, cómo, para qué, cuando y cuánto.

Para indagar si los objetivos están bien planteados, en la Guía de Administración del Riesgo del Departamento Administrativo de la Función Pública se plantea la necesidad de analizar su adecuada formulación, es decir, que contengan unos atributos mínimos, para lo cual puede sugiere hacer uso de las características SMART, cuya estructura se explica a continuación:

* S: Specific (específico): Lo importante es resolver cuestiones como: qué, cuándo, cómo, dónde, con qué, quién. Considerar el orden y los necesarios para el cumplimiento de la misión.
* M: Mensurable (Medible): Para ello es necesario involucrar algunos números en su definición por ejemplo porcentajes o cantidades exactas si aplica.
* A: Achievable: (Alcanzable): Para hacer alcanzable un objetivo se necesita un previo análisis de lo que se ha hecho y logrado hasta el momento. Esto ayudará a saber si lo que se propone es posible o como resultaría mejor.
* R: Relevant (Relevante): Considerar recursos, factores externos e información de actividades previas a fin de contar con elementos de juicio para su determinación.
* T: Timely(Temporal): Establecer un tiempo al objetivo ayudará a saber si lo que se esta haciendo es lo óptimo para llegar a la meta, así mismo permite determinar el cumplimiento y mediciones finales.

Fuente: Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

### Tipos de Riesgo

#### Riesgos de gestión:

Este tipo de riesgos pueden clasificarse así:

* Calidad: relacionados con los atributos de calidad establecidos en MIPG, las políticas de aseguramiento y control de calidad.
* Contractual: relacionado con los atrasos o incumplimientos de las etapas contractuales en cada vigencia.
* Comunicación: relacionado con los canales, medios y oportunidades para informar durante las diferentes etapas de un proyecto.
* Cumplimiento y conformidad: se asocian con los requisitos legales, contractuales, de ética pública y en general con su compromiso ante la comunidad.
* Estratégicos: asociado a la administración de la Entidad, a la misión y el cumplimiento de los objetivos estratégicos, la definición de políticas, y el diseño de lineamientos que respondan a las necesidades de los grupos de valor e interés
* Financieros: relacionado con el manejo de recursos, la ejecución presupuestal, la elaboración de los estados financieros, los pagos, manejos de excedentes de tesorería y el manejo de los bienes.
* Imagen: relacionado con la percepción y la confianza por parte de los grupos de valor frente a la Entidad
* Información: se asocia a la disponibilidad, confiabilidad e integridad de la información agregada y desagregada
* Integración: Se refiere a la integración de sistemas, áreas, entidades, etapas y elementos que se requieran coordinar para el desarrollo de un proyecto
* Operativos: riesgos provenientes del funcionamiento y operatividad de los procesos, sistemas de información, estructura de la entidad y articulación entre dependencias.
* Recurso Humano**:** Se asocia a la cualificación, competencia y disponibilidad de personal requerido para realizar un proyecto o función.

#### Riesgos de Corrupción:

Cuando por acción u omisión, mediante el uso indebido del poder, de los recursos o de la información, se lesionen los intereses de una entidad y en consecuencia, del Estado, para la obtención de un beneficio particular. Los riesgos de corrupción siempre deben gestionarse.

#### Tecnológicos y de seguridad digital:

Son los relacionados con la vulnerabilidad de la capacidad tecnológica para satisfacer las necesidades actuales y futuras y el cumplimiento de la misión de la entidad. Para profundizar consultar el numeral 5 del presente documento.

### Identificación de los puntos de riesgo:

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

### Identificación de áreas de impacto:

El área de impacto es la consecuencia económica o reputacional a la cual se ve expuesta la organización en caso de materializarse un riesgo. Los impactos que aplican son afectación económica (o presupuestal) y reputacional.

### Identificación de áreas de factores de riesgo:

Son las fuentes generadoras de riesgos. En la Tabla 2 se relaciona un listado con ejemplo de factores de riesgo que puede tener el INCI y que sugiere la Guía de Administración del Riesgo del Departamento Administrativo de la Función Pública.

Tabla No 2 Factores de Riesgo

| Factor | Definición | Descripción |
| --- | --- | --- |
| Procesos | Eventos relacionados con errores en las actividades que deben realizar los servidores de la entidad. | Falta de procedimientos |
| Errores de grabación, autorización |
| Errores en cálculos para pagos internos y externos |
| Falta de capacitación, temas relacionados con el personal |
| 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) |
| 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 |
| Factor | Definición | Descripción |
| Evento externo | Situaciones externas que afectan la entidad. | Suplantación de identidad |
| Asalto a la oficina |
| Atentados, vandalismo, orden público |

FUENTE: Guía para la administración del riesgo y el diseño de controles en entidades públicas del Departamento Administrativo de la Función Pública de Diciembre de 2020

### Descripción del riesgo:

La descripción del riesgo debe contener todos los detalles que sean necesarios y que sea fácil de entender tanto para el líder del proceso como para personas ajenas al mismo. La Guía propone una estructura que facilita su redacción y claridad que inicia con las palabras “Posibilidad de” y se analizan los siguientes aspectos:

Riesgo= Impacto (Qué) +Causa Inmediata (Cómo) +Causa Raíz (Por qué)

De la causa Raíz se desprenden la subcausa 1 y la subcausa 2 y los controles entran a atacar estas causas.

El Impacto + la causa inmediata es lo que puede ocurrir.

La anterior estructura evita la subjetividad en la redacción y permite entender la forma como se puede manifestar el riesgo, así como sus causas inmediatas y causas principales o raíz, esta es información esencial para la definición de controles en la etapa de valoración del riesgo.

A continuación se definen los componentes de la fórmula mencionada:

* Impacto: Son las consecuencias que puede ocasionar a la organización la materialización del riesgo.
* 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, es la base para la definición de controles en la etapa de valoración del riesgo. Se debe tener en cuenta que para un mismo riesgo pueden existir más de una causa o subcausas que pueden ser analizadas

### 2.7. Clasificación del riesgo:

Cada uno de los riesgos se clasifica de acuerdo con las siguientes categorías:

Tabla 3. Clasificación de los riesgos según categoría y relación con factores de riesgo:

| **Clasificación** | **Definición** | **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. | Están asociadas 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. | Están asociadas a varios factores |
| 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. | Infraestructura  Evento externo |

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas del Departamento Administrativo de la Función Pública de Diciembre de 2020

## **Valoración del riesgo**

### Análisis de riesgos:

Se busca establecer la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto

#### Determinación de la probabilidad:

La probabilidad es la posibilidad de ocurrencia del riesgo, la cual estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. De este modo, la probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año, o sea se determina la frecuencia con la que se lleva a cabo una actividad.

Tabla 4 Criterios para definir el nivel 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% |

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas del Departamento Administrativo de la Función Pública de Diciembre de 2020

#### Determinación del impacto:

Para la construcción de la tabla de criterios se definen los impactos económicos y reputacionales como las variables principales. En la versión del año 2018 de la Guía de administración del riesgo se contemplaban afectaciones a la ejecución presupuestal, pagos por sanciones económicas, indemnizaciones a terceros, sanciones por incumplimientos de tipo legal; así como afectación a la imagen institucional por vulneraciones a la información o por fallas en la prestación del servicio, todos estos temas se agrupan en impacto económico y reputacional en la versión 2020.

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

Tabla 5 Criterios para definir el nivel de impacto de los riesgos de gestión

|  |  |  |
| --- | --- | --- |
|  | Afectación Económica (o presupuestal) | Pérdida Reputacional |
| Leve 20% | Afectación menor a 10 SMLMV | El riesgo afecta la imagen de alguna 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 publicitarios sostenible a nivel país |

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas del Departamento Administrativo de la Función Pública de Diciembre de 2020

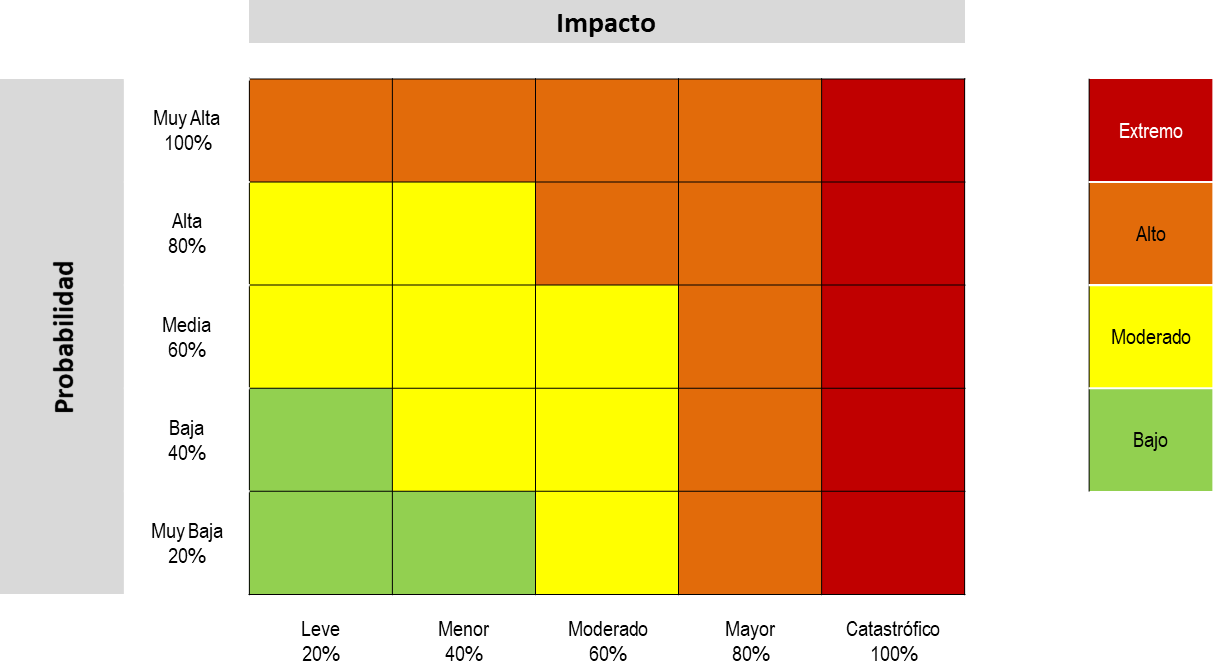
### Evaluación de riesgos:

A partir del análisis de la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto se determina la zona de riesgo inicial (RIESGO INHERENTE)

#### Análisis preliminar (riesgo inherente):

Se determinan los niveles de severidad a través de la ubicación del punto de intersección entre la probabilidad y el impacto. Se definen 4 zonas de severidad en la matriz de calor como se muestra en la figura 1

Figura 1 Matriz de calor (niveles de severidad del riesgo)



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas del Departamento Administrativo de la Función Pública de Diciembre de 2020

A continuación se cita un ejemplo de la Guía para la administración del riesgo y el diseño de controles en entidades públicas del Departamento Administrativo de la Función Pública de Diciembre de 2020, para mayor comprensión

Proceso: gestión de recursos

Objetivo: adquirir con oportunidad y calidad técnica los bienes y servicios requeridos por la entidad para su continua operación

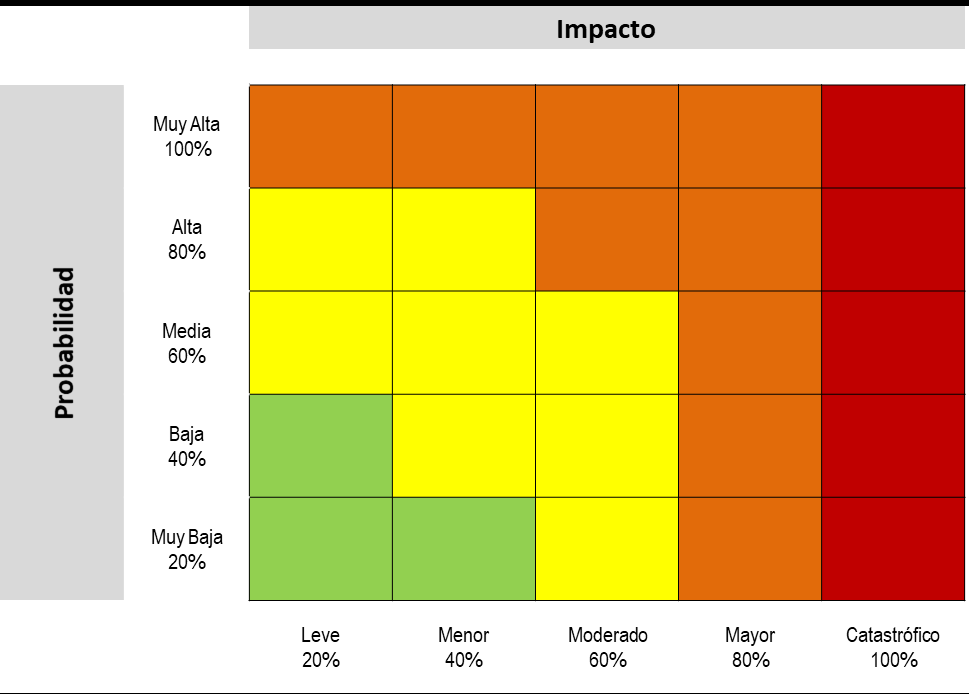
Riesgo identificado: posibilidad de afectación económica por multa y sanción del ente regulador debido a la adquisición de bienes y servicios sin el cumplimiento de los requisitos normativos

Probabilidad Inherente= moderada 60%

Impacto Inherente: mayor 80%

Aplicando la matriz de calor tenemos:

Cruzando los datos de probabilidad e impacto definidos (Punto de Intersección) se tiene zona de riesgo alta



#### Valoración de controles:

Un control es la medida que permite reducir o mitigar el riesgo. La identificación de controles se debe realizar a cada riesgo a través de las entrevistas con los líderes de procesos o servidores expertos en su quehacer y los responsables de implementar y monitorear los controles son los líderes de proceso con el apoyo de su equipo de trabajo.

##### Estructura para la descripción del control:

* 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.

##### Tipos de controles y los procesos:

* Control preventivo: control accionado en la entrada del proceso y antes de que se realice la actividad originadora del riesgo, se busca establecer las condiciones que aseguren el resultado final esperado.
* Control detectivo: control accionado durante la ejecución del proceso. Estos controles detectan el riesgo, pero generan reprocesos.
* Control correctivo: control accionado en la salida del proceso y después de que se materializa el riesgo. Estos controles tienen costos implícitos.

Así mismo, de acuerdo con la forma de ejecución se clasifican en:

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

##### Análisis y evaluación de los controles – Atributos:

Análisis de los atributos para el diseño del control, teniendo en cuenta características relacionadas con la eficiencia y la formalización.

Tabla 6 Atributos de para el diseño del control

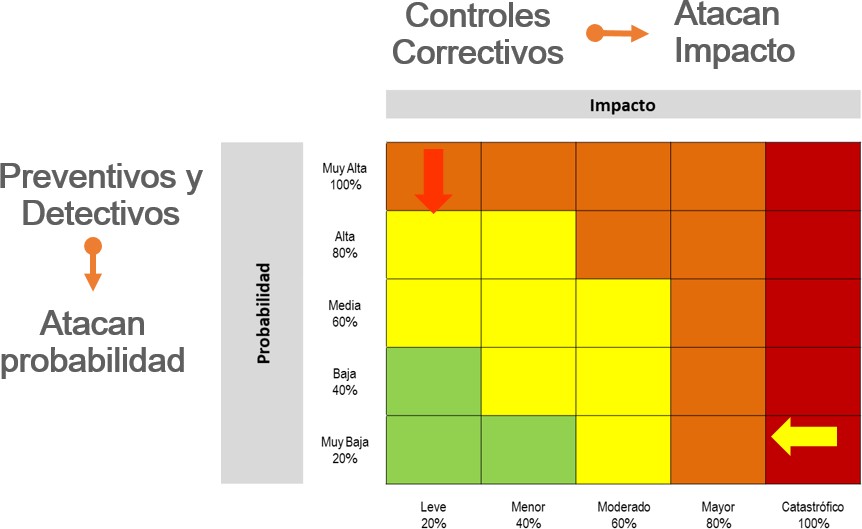
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Características | | | Descripción | Peso |
| Atributos de Eficiencia | Tipo | Preventivo | Va hacia las causas del riesgo, aseguran el resultado final esperado. | 25% |
| Detectivo | Detecta que algo ocurre y devuelve el proceso a los controles preventivos. 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 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 | - |
| Frecuencia | Continua | Este atributo identifica a los controles que se ejecutan siempre que se realiza la actividad originadora del riesgo. | - |
| Aleatoria | Este atributo identifica a los controles que no siempre se ejecutan cuando se realiza la actividad originadora del riesgo | - |
| 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 | - |

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas del Departamento Administrativo de la Función Pública de Diciembre de 2020

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

La siguiente figura muestra cuál es el movimiento en el eje de probabilidad y en el eje de impacto de acuerdo con los tipos de controles.

Figura 2 Movimiento en la matriz de calor acorde con el tipo de control



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas del Departamento Administrativo de la Función Pública de Diciembre de 2020

#### Nivel de riesgo (riesgo residual):

Es el resultado de aplicar la efectividad de los controles al riesgo inherente. Para la aplicación de los controles se debe tener en cuenta que estos mitigan el riesgo de forma acumulativa, esto quiere decir que una vez se aplica el valor de uno de los controles, el siguiente control se aplicará con el valor resultante luego de la aplicación del primer control.

Para facilitar la comprensión se continúa con el ejemplo que figura en la Guía para la administración del riesgo y el diseño de controles en entidades públicas del Departamento Administrativo de la Función Pública de Diciembre de 2020

Tabla 7 Controles y sus características

| Controles y sus características | | | | Peso |
| --- | --- | --- | --- | --- |
| Control 1:  El profesional del área de contratos verifica que la información suministrada por el proveedor corresponda con los requisitos establecidos de contratación a través de una lista de chequeo donde están los requisitos de información y la revisión con la información física suministrada por el proveedor, los contratos que cumplen son registrados en el Sistema de Información de Contratación | Tipo | Preventivo | X | 25% |
| Detectivo |  |  |
| Correctivo |  |  |
|  |
| Implementación | Automático |  |  |  |
|  |
| Manual | X | 15% |  |
|  |
| Documentación | Documentado | X | - |  |
| Sin documentar |  | - |  |
| Frecuencia | Continua | X | - |  |
|  |
| Aleatoria |  | - |  |
|  |
| Evidencia | Con registro | x |  |  |
| Sin registro |  | - |  |
| Total valoración control 1 |  |  |  | 40% |  |
| Control 2:  El jefe de contratos verifica en el sistema de información de contratación la información registrada por el profesional asignado y aprueba el proceso para la firma del ordenador del gasto. En el Sistema de información queda el registro correspondiente en caso de encontrar inconsistencias devuelve el proceso al profesional de contratos asifgnado | Tipo | Preventivo |  |  |  |
| Detectivo | X | 15% |  |
| Correctivo |  |  |  |
| Implementación | Automático |  |  |  |
| Manual | X | 15% |  |
|  |
| Documentación | Documentado | X | - |  |
| Sin documentar |  | - |  |
| Frecuencia | Continua | X | - |  |
|  |
| Aleatoria |  | - |  |
| Evidencia | Con registro | X | - |  |
| Sin registro |  | - |  |
| Total valoración control 2 |  |  |  | 30% |  |

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas del Departamento Administrativo de la Función Pública de Diciembre de 2020

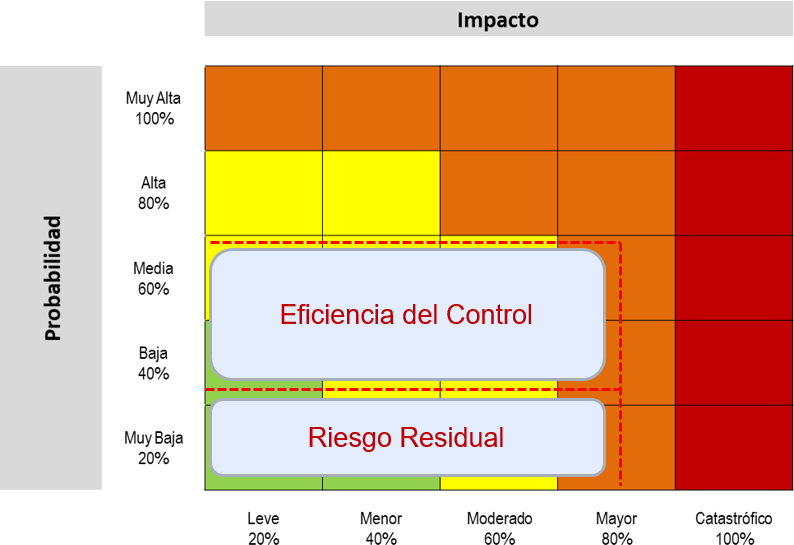
A continuación se muestra el riesgo con los datos de los controles para establecer el riesgo residual

Tabla 8 Riesgo con los datos de los controles para establecer el riesgo residual

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Riesgo | Datos relacionados con la probabilidad e impacto inherentes | | Datos valoración de controles | | Cálculos requeridos |
| Posibilidad de  pérdida económica por multa y sanción del ente regulador debido a la  adquisición de  bienes y servicios sin el cumplimiento de los requisitos normativos | Probabilidad inherente | 60% | Valoración control 1  preventivo | 40% | 60%\* 40% = 24%  60% - 24% = 36% |
| Valor probabilidad para aplicar 2º control | 36% | Valoración control 2 detectivo | 30% | 36%\* 30% = 10,8%  36% - 10,8% =  25,2% |
| Probabilidad Residual | 25,2 % |  |  |  |
| Impacto Inherente | 80% |  |  |  |
| No se tienen controles para aplicar al impacto | N/A | N/A | N/A | N/A |
| Impacto Residual | 80% |  |  |  |

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas del Departamento Administrativo de la Función Pública de Diciembre de 2020

Movimiento en la matriz según el ejemplo propuesto



Nota: En caso de no contar con controles correctivos, el impacto residual es el mismo calculado inicialmente, es importante señalar que no será posible su movimiento en la matriz para el impacto.

### Estrategias para combatir el riesgo:

Es la 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, esto para procesos en funcionamiento, cuando se trate de procesos nuevos, se procede a partir del riesgo inherente.

* Reducir: Después de realizar un análisis y considerar que el nivel del riesgo es alto se determina tratarlo mediante transferencia o mitigación y al elaborar el plan de acción este se convierte en una herramienta de planificación empleada para la gestión y control de tareas o proyectos y debe contemplar un responsable, la fecha de implementación y una fecha de seguimiento.
* Mitigar: Después de realizar un análisis y considerar los niveles de riesgo se implementan acciones que mitiguen el nivel de riesgo. No necesariamente es un control adicional.
* Transferir: Después de realizar un análisis, se considera que la mejor estrategia es tercerizar el proceso o trasladar el riesgo a través de seguros o pólizas. La responsabilidad económica recae sobre el tercero, pero no se transfiere la responsabilidad sobre el tema reputacional.
* Aceptar: Después de realizar un análisis y considerar los niveles de riesgo se determina asumir el mismo conociendo los efectos de su posible materialización.
* Evitar: Después de realizar un análisis y considerar que el nivel del riesgo es demasiado alto, se determina NO asumir la actividad que genera este riesgo.

### Monitoreo y revisión:

El Modelo Integrado de Planeación y Gestión (MIPG) en la dimensión 7 “Control interno” desarrolla a través de las líneas de defensa la responsabilidad de la gestión del riesgo y control.

Después de la publicación y durante el respectivo año de vigencia, se podrán realizar los ajustes y las modificaciones necesarias orientadas a mejorar el mapa de riesgos de gestión. En este caso, deberán dejarse por escrito los ajustes, modificaciones o inclusiones realizadas. *La Guía de la administración del riesgo y el diseño de controles en entidades públicas del Departamento Administrativo de la Función Pública del mes de Diciembre de 2020 en la página 52, sugiere un formato para documentar la metodología explicada hasta el momento.*

Monitoreo: en concordancia con la cultura del autocontrol al interior del INCI, los líderes de los procesos junto con su equipo deben realizar monitoreo y evaluación permanente a la gestión de riesgos de gestión y documentarlo cada cuatro meses.

Seguimiento: el jefe de control interno, o quien haga sus veces, debe adelantar seguimiento a la gestión de riesgos de gestión. En este sentido, es necesario que en sus procesos de auditoría interna analicen las causas, los riesgos y la efectividad de los controles incorporados en el mapa de riesgos.

A continuación se detallan los roles y responsabilidades de todos los actores de la gestión del riesgo y el control en la entidad para proporcionar aseguramiento de la gestión y previniendo la materialización.

#### ROLES DE LAS LÍNEAS DE DEFENSA EN LA GESTIÓN DEL RIESGO

##### ESTRATÉGICA: ALTA DIRECCIÓN Y COMITÉ INSTITUCIONAL DE COORDINACIÓN DE CONTROL INTERNO:

* Establecer y aprobar la política de administración del riesgo la cual incluye los niveles de aceptación o tolerancia al riesgo.
* Supervisar el cumplimiento de la política de administración del riesgo
* Revisar el adecuado análisis y articulación de los objetivos institucionales con los objetivos de los procesos que sirvieron de base para llevar a cabo la identificación de los riesgos.
* Analizar los cambios en el entorno (contexto interno y externo) que puedan tener un impacto significativo en la operación de la entidad y que puedan generar cambios en la estructura de riesgos y controles
* Realizar seguimiento y análisis periódico a los riesgos institucionales
* Retroalimentar al Comité Institucional de Gestión y Desempeño sobre los ajustes que se deban hacer frente a la gestión del riesgo
* Evaluar el estado del sistema de control interno y aprobar las modificaciones, actualizaciones y acciones de fortalecimiento del mismo.

##### PRIMERA LÍNEA: GERENTES PÚBLICOS Y LIDERES DE PROCESO, PROGRAMA O PROYECTO:

* Identificar, analizar, valorar, monitorear y evaluar los riesgos que pueden afectar los proyectos, planes y procesos a su cargo y actualizarlo cuando se requiera.
* Orientar el desarrollo e implementación de políticas y procedimientos y asegurar que sean compatibles con las metas y objetivos de la entidad y emprender las acciones de mejora para su logro.
* Diseñar, implementar y monitorear los controles además de gestionar de manera directa en el día a día los riesgos de la entidad.
* Definir, aplicar y hacer seguimiento a los controles para mitigar los riesgos identificados y proponer mejoras a la gestión del riesgo de los procesos.
* Supervisar la ejecución de los controles aplicados por el equipo de trabajo en la gestión del día a día, detectar las deficiencias de los controles y determinar las acciones de mejora a que haya lugar
* Desarrollar ejercicios de autoevaluación para establecer la eficiencia, eficacia y efectividad de los controles
* Informar a la oficina de planeación (segunda línea) sobre los riesgos materializados en los proyectos, planes y/o procesos a su cargo
* Reportar a la Oficina de Planeación, los avances y evidencias de la gestión de los riesgos a cargo del proceso asociado.

##### SEGUNDA LÍNEA:OFICINA ASESORA DE PLANEACIÓN, SUPERVISORES DE CONTRATOS, COORDINADORES DE OTROS SISTEMAS DE GESTIÓN Y COMITÉS INSTITUCIONALES

* Asesorar a la línea estratégica en el análisis del contexto interno y externo, para la definición y aplicación de la política de riesgo, el establecimiento de los niveles de impacto y el nivel de aceptación del riesgo.
* Consolidar el Mapa de riesgos institucional (riesgos de mayor criticidad frente al logro de los objetivos) y presentarlo para análisis y seguimiento ante el Comité Institucional de Gestión y Desempeño.
* Presentar al Comité Institucional de Control Interno, el seguimiento a la eficacia de los controles en las áreas identificadas en los diferentes niveles de operación de la entidad.
* Acompañar, orientar y entrenar a los líderes de procesos en la identificación, análisis y valoración del riesgo.
* Monitorear los controles establecidos por la primera línea de defensa acorde con la información suministrada por los líderes de procesos.
* Supervisar en coordinación con los demás responsables de esta segunda línea de defensa que la primera línea identifique, evalué y gestione los riesgos y controles para que se generen acciones.
* Evaluar que los riesgos sean consistentes con la presente política de la entidad y que sean monitoreados por la primera línea de defensa.
* Promover ejercicios de autoevaluación para establecer la eficiencia, eficacia y efectividad de los controles.
* Identificar cambios en los riesgos, especialmente aquellos ubicados en zona baja y presentarlo para aprobación del Comité Institucional de Coordinación de Control Interno.

##### TERCERA LÍNEA: OFICINA DE CONTROL INTERNO

* Realizar evaluación independiente al cumplimiento y efectividad de la Política de Administración del Riesgo, los mecanismos de evaluación del riesgo y la efectividad de los controles, en cumplimiento de su rol “Evaluación de la Gestión del Riesgo”.
* Alertar sobre probabilidad de riesgo de fraude o corrupción en áreas auditadas.
* Evaluar la efectividad y la aplicación de controles, planes de contingencia y actividades de monitoreo vinculadas a los cambios que pueden afectar el Sistema de Control Interno para el cumplimiento de los objetivos.
* Proporcionar aseguramiento objetivo sobre la eficacia de la gestión del riesgo y control, con énfasis en el diseño e idoneidad de los controles establecidos en los procesos.
* Proporcionar aseguramiento objetivo en las áreas identificadas no cubiertas por la segunda línea de defensa.
* Asesorar 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.
* Llevar a cabo el seguimiento a los riesgos consolidados en los mapas de riesgos de conformidad con el Plan Anual de Auditoria y reportar los resultados al Comité Institucional de Coordinación de Control Interno

## **LINEAMIENTOS SOBRE RIESGOS RELACIONADOS CON POSIBLES ACTOS DE CORRUPCIÓN**

### 

En el marco del Plan Anticorrupción y de Atención al Ciudadano establecido en la Ley 1474 de 2011 (artículo 73) y el Decreto 124 de 2016 (artículo 2.1.4.1.) que define las estrategias de lucha contra la corrupción y de atención al ciudadano se definen los lineamientos para la identificación y valoración de riesgos de corrupción que hacen parte del componente 1 “Gestión del riesgo de corrupción”.

El riesgo de corrupción se define como la posibilidad de que por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado, se establece anualmente por procesos y se debe describir de manera clara y precisa.

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 de corrupción. En este caso, deberán dejarse por escrito los ajustes, modificaciones o inclusiones realizadas.

Monitoreo: en concordancia con la cultura del autocontrol al interior del INCI, los líderes de los procesos junto con su equipo deben realizar monitoreo y evaluación permanente a la gestión de riesgos de corrupción y documentarlo cada cuatro meses.

Seguimiento: el jefe de control interno, o quien haga sus veces, debe adelantar seguimiento a la gestión de riesgos de corrupción. En este sentido, es necesario que en sus procesos de auditoría interna analicen las causas, los riesgos de corrupción y la efectividad de los controles incorporados en el mapa de riesgos de corrupción.

Teniendo en cuenta la criticidad del tema y que se requiere su publicación en página web, se podrá anonimizar la información relacionada con los controles establecidos que pueden tener relación con información clasificada o reservada.

### Identificación del riesgo de corrupción

A manera de ilustración a continuación se señalan algunos de los procesos, procedimientos o actividades susceptibles de actos de corrupción, a partir de los cuales la entidad podrá adelantar el análisis de contexto interno para la correspondiente identificación de los riesgos:

**Direccionamiento estratégico:**

* Concentración de autoridad o exceso de poder o Extralimitación de funciones.
* Ausencia de canales de comunicación.
* Amiguismo y clientelismo.

**Financiero**

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

**Contratación:**

* Estudios previos o de factibilidad deficientes.
* Estudios previos o de factibilidad manipulados por personal interesado en el futuro proceso de contratación. (Estableciendo necesidades inexistentes o aspectos que benefician a una firma en particular).
* Pliegos de condiciones hechos a la medida de una firma en particular.
* Disposiciones establecidas en los pliegos de condiciones que permiten a los participantes direccionar los procesos hacia un grupo en particular. (Ej.: media geométrica).
* Visitas obligatorias establecidas en el pliego de condiciones que restringen la participación.
* Adendas que cambian condiciones generales del proceso para favorecer a grupos determinados.
* Urgencia manifiesta inexistente.
* Concentrar las labores de supervisión en poco personal.
* Contratar con compañías de papel que no cuentan con experiencia

**Comunicación y gestión documental:**

* Ausencia o debilidad de medidas y/o políticas de conflictos de interés.
* Concentración de información de determinadas actividades o procesos en una persona.
* Ausencia de sistemas de información que pueden facilitar el acceso a información y su posible manipulación o adulteración.
* Ocultar la información considerada pública para los usuarios.
* Ausencia o debilidad de canales de comunicación

**Gestión Humana- Procesos Disciplinarios**

* Inexistencia de canales de denuncia interna o externa.
* Dilatar el proceso para lograr el vencimiento de términos o la prescripción de este.
* Desconocimiento de la ley mediante interpretaciones subjetivas de las normas vigentes para evitar o postergar su aplicación.
* Exceder las facultades legales en los fallos

Fuente: Secretaría de Transparencia, 2018

#### Lineamientos para la identificación del riesgo de corrupción

Las preguntas clave para la identificación del riesgo son:

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

Si en la descripción del riesgo, se cumplen las siguientes condiciones se trata de un riesgo de corrupción:

* Acción u omisión
* Uso del Poder
* Desviar la gestión de lo público
* Beneficio privado

## **Valoración del riesgo**

#### Determinación de la probabilidad

La determinación de la probabilidad (posibilidad de ocurrencia del riesgo) se debe llevar a cabo de acuerdo con lo establecido en el aparte 3.1.1 de esta guía.

#### Determinación del impacto

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.

Para calificar el **impacto** a los **riesgos de corrupción** se debe partir del caso hipotético de la materialización del riesgo y tener en cuentael siguiente cuestionario, iniciando con la pregunta: “Si el riesgo se materializa podría:

1. Afectar al 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 pérdida de recursos económicos
7. Afectar la generación de los productos o la prestación de servicios
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 pérdida de vidas humanas
17. Afectar la imagen regional
18. Afectar la imagen nacional
19. Generar daño ambiental

* Si menos de cinco (5) respuestas son afirmativas la calificación del impacto es **moderado**, lo cual genera medianas consecuencias sobre la entidad
* Si el número de respuestas afirmativas esta entre seis (6) y once (11) el impacto es **mayor** y se generan altas consecuencias para la entidad.
* Si el número de respuestas afirmativas es mayor a doce (12) el impacto es **catastrófico** y se generan consecuencias desastrosas para la entidad

#### 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 que soló se presenta impacto moderado, mayor o catastrófico como se dijo anteriormente

#### Valoración de controles

La valoración de los controles existentes establecido en el numeral 3.2.2, así como las demás disposiciones contenidas en el capítulo 3 de esta guía, son aplicables a la gestión del riesgo de corrupción.

La Guía de la administración del riesgo y el diseño de controles en entidades públicas del Departamento Administrativo de la Función Pública del mes de Diciembre de 2020 en la página 75, sugiere un formato para documentar la metodología explicada hasta el momento.

## **LINEAMIENTOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN**

La política de seguridad digital se vincula al modelo de seguridad y privacidad de la información, 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.

### 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.

Un activo es cualquier elemento que tenga valor para la organización, 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 organización para funcionar en el entorno digital

La identificación de los activos 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

Pasos para la identificación de activos

* Paso 1: Listar los activos por proceso
* Paso 2: Identificar el dueño de los activos
* Paso3: Clasificar los activos
* Paso 4: Clasificar la información
* Paso 5: Determinar la criticidad del activo
* Paso 6: Identificar si existe infraestructura crítica cibernética

Fuente: Elaboración conjunta entre la Dirección de Gestión y Desempeño Institucional de Función Pública y el Ministerio TIC, 2018.

### Identificación del riesgo:

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

1. Pérdida de la confidencialidad
2. Pérdida de la integridad
3. 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](https://www.funcionpublica.gov.co/documents/418548/34316316/Anexo%2B4%2BLineamientos%2Bpara%2Bla%2BGestion%2Bdel%2BRiesgo%2Bde%2B%2BSeguridad%2BDigital%2Ben%2BEntidades%2BPúblicas%2B-%2BGuía%2Briesgos%2B2018.pdf/1ce5099d-c5e5-8ba2-00bc-58f801d3657b) [para entidades públicas](https://www.funcionpublica.gov.co/documents/418548/34316316/Anexo%2B4%2BLineamientos%2Bpara%2Bla%2BGestion%2Bdel%2BRiesgo%2Bde%2B%2BSeguridad%2BDigital%2Ben%2BEntidades%2BPúblicas%2B-%2BGuía%2Briesgos%2B2018.pdf/1ce5099d-c5e5-8ba2-00bc-58f801d3657b) 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

Nota: 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.

Tabla 9 Tabla de amenazas y vulnerabilidades de acuerdo con el tipo de activo

|  |  |  |
| --- | --- | --- |
| Tipo de activo | Ejemplos de vulnerabilidades | Ejemplos de amenazas |
| Hardware | Almacenamiento de medios sin protección | Hurto de medios o documentos |
| Software | Ausencia de parches de seguridad | Abuso de los derechos |
| Red | Líneas de comunicación sin protección | Escucha encubierta |
| Información | Falta de controles de acceso físico | Hurto de información |
| Tipo de activo | Ejemplos de vulnerabilidades | Ejemplos de amenazas |
| Personal | Falta de capacitación en las herramientas | Error en el uso |
| Organización | Ausencia de políticas de seguridad | Abuso de los derechos |

Fuente: Ministerio de Tecnologías de la Información y Comunicaciones Min TIC, 2018.

### Valoración del riesgo:

Para esta etapa se asociarán las tablas de probabilidad e impacto definidas en la primera parte de la presente guía.

Para el análisis preliminar (riesgo inherente), en esta etapa se define el nivel de severidad para el riesgo de seguridad de la información identificado, para ello se aplica la matriz de calor establecida en el numeral 3.2.1

### Controles asociados a la seguridad de la información

Las entidades públicas podrán mitigar/tratar los riesgos de seguridad de la información empleando como mínimo los controles del Anexo A de la ISO/IEC 27001:2013, estos controles se encuentran en el anexo 4. “Modelo Nacional de Gestión de riesgo de seguridad de la Información en entidades públicas”, siempre y cuando se ajusten al análisis de riesgos.

Acorde con el control seleccionado, será necesario considerar las características de diseño y ejecución definidas para su valoración.

A continuación se incluyen algunos ejemplos de controles y los dominios a los que pertenecen, la lista completa se encuentra en del documento maestro del modelo de seguridad y privacidad de la información (MSPI):

Tabla 10 Controles para riesgos de seguridad de la información

|  |  |
| --- | --- |
| Procedimientos operacionales y  responsabilidades | Objetivo: asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información |
| Procedimientos de operación  documentados | Control: los procedimientos de operación se deberían documentar y poner a disposición de todos los usuarios que los necesiten. |
| Gestión de cambios | Control: se deberían controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información. |
| Gestión de capacidad | Control: para asegurar el desempeño requerido del sistema se debería hacer seguimiento al uso de los recursos, llevar a cabo los ajustes y las proyecciones de los requisitos sobre la capacidad futura. |
| Separación de los ambientes de  desarrollo, pruebas y operación | Control: se deberían separar los ambientes de desarrollo, prueba y operación para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación. |
| Protección contra códigos maliciosos | Objetivo: asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos. |
| Controles contra códigos maliciosos | Control: se deberían implementar controles de detección, prevención y recuperación, combinados con la toma de conciencia apropiada por parte de los usuarios para protegerse contra códigos maliciosos. |
| Copias de respaldo | Objetivo: proteger la información contra la perdida de datos. |
| Respaldo de información | Control: se deberían hacer copias de respaldo de la información, del software y de las imágenes de los sistemas, ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada. |

NOTA: La guía de administración del riesgo incluye el formato para documentar los riesgos seguridad digital en la página 89

## **NIVELES DE ACEPTACIÓN DEL RIESGO:**

## Tabla 11

| **Zona de riesgo** | **Significado** | **Nivel de aceptación** | **Tratamiento** |
| --- | --- | --- | --- |
| Extrema | En caso de materializarse, el riesgo genera impactos graves significativos para la Entidad. | No aceptable | Las acciones que se emprendan para tratar el riesgo extremo deben orientarse a evitar, reducir, compartir o transferir el riesgo. |
| Alta | En caso de materializarse, el riesgo genera impactos graves para la Entidad. | No aceptable | Considerando el impacto de estos riesgos, las acciones deben estar enfocadas a evitar, reducir, compartir o transferir el riesgo. |
| Moderada | En caso de materializarse, el riesgo genera impactos mínimos para la Entidad. | No aceptable | Las acciones deben estar enfocadas a reducir la probabilidad de ocurrencia del riesgo. |
| Baja | En caso de materializarse, el riesgo genera impactos sustancialmente leves para la Entidad. | Aceptable | El riesgo catalogado en nivel bajo se asume y es necesario realizar seguimiento continuo del riesgo. |

Fuente: Guía para la Gestión del Riesgo y diseño de controles en entidades públicas del Departamento Administrativo de la Función Pública 2020.

## **ACCIONAR ANTE LOS RIESGOS MATERIALIZADOS**

El Departamento Administrativo de la Función Pública ha establecido unos lineamientos para tratar el riesgo materializado, los cuales involucran a la Asesoría de Control Interno y a los líderes de los procesos y se encuentran en la siguiente tabla:

Tabla 12

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Detectado por** | **Riesgo de corrupción** | **Riesgo de gestión** | | | |
|
| **Zona extrema** | **Zona alta** | **Zona moderada** | **Zona baja** |
| Oficina de Control Interno | 1. Convocar al Comité de Coordinación de Control Interno e informar sobre los hechos detectados, desde donde se tomarán las decisiones para iniciar la investigación de los hechos. | 1.          Informar al líder del proceso sobre el hecho encontrado. | | | 1. Informar al líder del proceso sobre el hecho. |
| 2. Dependiendo del alcance (normatividad asociada al hecho de corrupción materializado), realizar la denuncia ante el ente de control respectivo. | 2.          Orientar al líder del proceso para que realice la revisión, análisis y acciones correspondientes para resolver el hecho. | | |  |
| 3.          Facilitar el inicio de las acciones correspondientes con el líder del proceso, para revisar el mapa de riesgos y sus controles asociados. | 3.          Verificar que se tomaron las acciones y que se actualizó el mapa de riesgos correspondiente. | | | 2. Orientar técnicamente sobre las acciones determinadas en la política de riesgos institucional. |
| 4.          Verificar que se tomaron las acciones y se actualizó el mapa de riesgos. | 4.          Convocar al Comité de Coordinación de Control Interno e informar sobre la actualización realizada. | | |  |

Fuente: Guía para la Administración del Riesgo, Departamento Administrativo de la Función Pública 2020

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  |  |  | | | |
| **Detectado por** | **Riesgo de corrupción** | **Riesgo de gestión** | | | |
| **Zona extrema** | **Zona alta** | **Zona moderada** | **Zona baja** |
| Líder del proceso u otro(s) funcionario(s) que participa(n) o interactúa(n) con el proceso | 1. Informar a la Alta Dirección sobre el hecho encontrado. 2. De considerarlo necesario, realizar la denuncia ante el ente de control respectivo 3. Iniciar con las acciones correctivas necesarias. 4. Realizar el análisis de causas y determinar acciones preventivas y de mejora.   5. Análisis y actualización del mapa de riesgos. | 1. Tomar las acciones correctivas necesarias, dependiendo del riesgo materializado. 2. Iniciar el análisis de causas y determinar acciones preventivas y de mejora. 3. Analizar y actualizar el mapa de riesgos. 4. Informar a la Alta Dirección sobre el hallazgo y las acciones tomadas. | | | Aplicar las orientaciones de la política de riesgos institucional.    (Verificar los niveles de aceptación del riesgo). |

Fuente: Guía para la Administración del Riesgo, Departamento Administrativo de la Función Pública 2020

# Referencias

DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA, Guía para la administración del riesgo y el diseño de controles en entidades públicas Diciembre de 2020, VERSIÓN 5 DIRECCIÓN DE GESTIÓN Y DESEMPEÑO INSTITUCIONAL,

1. https://www.funcionpublica.gov.co/web/eva/biblioteca-virtual/-/document\_library/bGsp2IjUBdeu/view\_file/34316499 [↑](#footnote-ref-1)