Acuerdo Nº 022
(30 de Agosto de 2021)

"Por el cual se deroga el Acuerdo No. 018 del 27 de noviembre de 2019 y se establece la Política para la Administración de Riesgos en el Instituto Superior de Educación Rural ISER de Pamplona."

EL CONSEJO DIRECTIVO DEL INSTITUTO SUPERIOR DE EDUCACIÓN RURAL ISER DE PAMPLONA

En uso de sus facultades legales y estatutaria, en especial las que le confiere el acuerdo número 010 del 02 de diciembre de 1993- Estatuto General- Articulo 14 literal a y

CONSIDERANDO

Que el literal f) del artículo 2º de la Ley 87 de 1993, establece como uno de los objetivos del Sistema de Control Interno, la definición y aplicación de las medidas para prevenir los riesgos, detectar y corregir las desviaciones que se presenten en la organización y que puede afectar el logro de sus objetivos.

Que, según la Ley 87 de 1993, conforme con el artículo 1º, parágrafo único, los manuales de procedimientos son instrumentos a través de los cuales se cumple el control interno.

Que, mediante el Decreto 1537 de 2001 se reglamentó parcialmente la Ley 87 de 1993, y en el artículo 4 señala la administración de riesgos "*Como parte integral del fortalecimiento de los sistemas de control interno en las entidades públicas las autoridades correspondientes establecerán y aplicarán políticas de administración del riesgo. Para tal efecto, la identificación y análisis de riesgo debe ser un proceso permanente e interactivo entre la administración y las oficinas de control interno o quienes haga sus veces, evaluando los aspectos tanto internos como externos que pueden llegar a representar amenaza para consecución de los objetivos organizaciones, con miras a establecer acciones efectivas, representadas en actividades de control, acordadas entre los responsables de las áreas o procesos y las oficinas de control interno e integradas de manera inherente los procedimientos*".

Que, el Decreto 2641 de 2012, en el artículo 1º, señala como metodología para diseñar y hacer seguimiento a la estrategia de lucha contra la corrupción y de atención al ciudadano de que trata el artículo 73 de la Ley 1474 de 2011, la establecida en el Plan Anticorrupción y de Atención al Ciudadano, en cuyo primer componente incorpora la "Metodología para la identificación de riesgos de corrupción y acciones para su manejo".

Que, el Decreto 124 de 2016, en su artículo 2.1.4.1 y 2.1.4.2, establece la Estrategia de lucha contra la corrupción y de Atención al Ciudadano. Señalando como metodología para diseñar y hacer seguimiento a la estrategia de lucha contra la corrupción y de atención al ciudadano – Mapas de Riesgo de Corrupción de que trata el artículo 73 de la Ley 1474 de 2011, la establecida en el Plan Anticorrupción y de Atención al Ciudadano contenida en el documento "Estrategias para la Construcción del Plan Anticorrupción y de Atención al Ciudadano-Versión 2".

Que, mediante Acuerdo No. 018 del 27 de noviembre de 2019 se "aprueba la Política para la Gestión Integral del Riesgo en el Instituto Superior de Educación Rural ISER de Pamplona", la cual estaba basada en la "Guía para la administración de Riesgos de Gestión, Corrupción y Seguridad Digital y el Diseño de Controles en Entidades Públicas versión 4".

Que, el Departamento Administrativo de la Función Pública, publicó la "Guía para la administración de Riesgos y el Diseño de Controles en Entidades Públicas versión 5", en diciembre de 2020 en la que "se actualizaron y precisaron algunos elementos metodológicos para mejorar el ejercicio de identificación y valoración del riesgo" y define que "para la implementación de la gestión del riesgo, es necesario que cada entidad haga un análisis de las estrategias, la formulación de objetivos y la implementación de esos objetivos en la toma de decisiones cotidiana, lo que permitirá una identificación del riesgo adecuada a las necesidades de cada organización, con un enfoque preventivo que permita la protección de los recursos, alcanzar mejores resultados y mejorar la prestación de servicios a sus usuarios aspectos fundamentales frente a la generación de valor público, eje fundamental en el que hacer de todas las organizaciones públicas".

Que, la propuesta de la Política para la Administración de Riesgos en del Instituto Superior de Educación Rural ISER de Pamplona, fue presentada por la Alta Dirección al Comité de Coordinación de Control Interno, conforme al componente de institucionalidad bajo el cual funciona el Modelo Integrado de Planeación y Gestión, adoptado mediante Resolución No. 100 del 15 de febrero de 2021.

En mérito de lo expuesto,

ACUERDA

ARTÍCULO PRIMERO. Derogar el Acuerdo No. 018 del 27 de noviembre de 2019 "Por el cual se aprueba la Política para la Gestión Integral del Riesgo en el Instituto Superior de Educación Rural ISER de Pamplona".

ARTÍCULO SEGUNDO. Establecer la Política para la Administración de Riesgos en el Instituto Superior de Educación Rural ISER de Pamplona, la cual quedará de la siguiente manera:

PRESENTACIÓN

El Instituto Superior de Educación Rural ISER de Pamplona, define su política para la Administración de Riesgos tomando como referente los parámetros del Modelo Integrado de Planeación y Gestión (MIPG) en los procesos, así como los del Modelo Estándar de Control Interno (MECI), en lo concerniente a las líneas de defensa y las directrices de la Guía para la administración de Riesgos y el Diseño de Controles en Entidades Públicas versión 5 del Departamento Administrativo de la Función Pública – DAFP, la cual articula los riesgos de gestión, corrupción y de seguridad de la información y la estructura del Sistema Integrado de Gestión – SGI en el requisito de Planificación de Riesgos.

OBJETIVO

Orientar a los líderes de procesos del Instituto Superior de Educación Rural sobre las acciones que se deben adelantar, encaminadas a disminuir la probabilidad de ocurrencia y posible impacto de todas aquellas situaciones que puedan entorpecer el propósito de alcanzar de manera eficaz y efectiva el logro de los objetivos y la misión institucional, mediante la identificación, el monitoreo, seguimiento y evaluación del riesgo en los periodos de tiempos establecidos en esta política.

1. ÁMBITO DE APLICACIÓN

La política para la Administración de Riesgos aplica para los planes, programas, procesos y acciones ejecutadas por los líderes de procesos y servidores durante el ejercicio de sus funciones, que inicia desde el establecimiento del contexto, la identificación de los riesgos, evaluación, implementación de los controles y acciones que minimicen el impacto o la probabilidad de ocurrencia de estos, hasta el monitoreo, seguimiento y comunicación.

2. TERMINOS Y DEFINICIONES

Definiciones tomadas de la Norma NTC-ISO 31000 (ICONTEC 2018) y de la nueva guía de administraciones del riesgo y diseño de controles en Entidades Públicas (publicada por el DAFP en el 2020).

- **Activo:** En el contexto de seguridad digital son elementos tales como aplicaciones de la organización, servicios web, redes, Hardware, información digital 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.
- **Causa:** Todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.
- **Consecuencia:** Los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas.

- **Causa inmediata:** Circunstancias bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo.
- **Causa Raíz:** Causa principal o básica, corresponde a las razones por la cuales se puede presentar el riesgo.
- **Factores de Riesgo:** Son las fuentes generadoras de riesgos.
- **Disponibilidad:** Propiedad de ser accesible y utilizable a demanda por una entidad.
- **Confidencialidad:** Propiedad de la información que la hace no disponible, es decir, divulgada a individuos, entidades o procesos no autorizados.
- **Control:** Son las políticas, procesos, dispositivos, prácticas y otras acciones que actúan para eliminar o minimizar los riesgos, adversos o mejorar oportunidades positivas. Proveen una seguridad razonable relativa al logro de los objetivos.
- **Identificación del riesgo:** Proceso que determina que puede suceder, por qué y el cómo.
- **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.
- **Apetito de riesgo:** Es el nivel de riesgo que la entidad puede aceptar, relacionado con sus Objetivos, el marco legal y las disposiciones de la Alta Dirección y del Órgano de Gobierno. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.
- **Capacidad de riesgo:** Es el máximo valor del nivel de riesgo que una Entidad puede soportar y a partir del cual se considera por la Alta Dirección y el Órgano de Gobierno que no sería posible el logro de los objetivos de la Entidad.
- **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.
- **Riesgo:** Es toda posibilidad de ocurrencia de una situación que pueda entorpecer el normal desarrollo de las funciones de la entidad y le impidan el logro de sus objetivos.
- **Riesgo de Gestión:** Posibilidad de que suceda algún evento que tendrá un impacto sobre cumplimiento de los objetivos. Se expresa en términos de probabilidad y consecuencias.
- **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:** Es aquel al que se enfrenta una entidad en ausencia de acciones de la dirección para modificar su probabilidad o impacto.
- **Riesgo Residual:** Nivel de riesgo que permanece luego de tomar medidas de tratamiento de riesgo.
- **Tolerancia al riesgo:** son los niveles aceptables de desviación relativa a la consecución de objetivos. Pueden medirse y a menudo resulta mejor, con las mismas unidades que los objetivos correspondientes. Para el riesgo de corrupción la tolerancia es inaceptable.

- **Probabilidad:** se entiende como la posibilidad de ocurrencia del riesgo. Esta puede ser medida con criterios de frecuencia o factibilidad.
- **Impacto:** Se entiende como las consecuencias que puede ocasionar a la organización la materialización del riesgo.
- **Valoración del Riesgo:** Es el conjunto de procesos que permiten analizar y evaluar el riesgo.
- **Vulnerabilidad:** Es una debilidad, atributo, causa o falta de control que permitiría la explotación por parte de una o más amenazas contra los activos.

3. ROLES Y RESPONSABILIDADES:

Línea Estratégica:

- **Comité de Coordinación de Control Interno**:

✓ Someter a aprobación del representante legal la política de administración del riesgo y hacer seguimiento, en especial a la prevención y detección de fraude y mala conducta.
✓ Retroalimentar a la alta dirección sobre la efectividad de los controles para la gestión del riesgo y hacer seguimiento a su administración. Establecer y aprobar la Política de Administración del Riesgo.

Primera Línea de Defensa: (Líderes de proceso):

✓ Revisar junto con su equipo el ejercicio de autocontrol de trabajo y el adecuado diseño y ejecución de sus controles, documentándolos en sus procedimientos.
✓ A corte 30 de abril, agosto 31 y diciembre 31 la primera línea de defensa deberá reportar el seguimiento al cumplimiento de los controles y las acciones si estas aplican.
✓ Cuatrimestralmente revisar el cumplimiento de los objetivos de su proceso e indicadores asociados y establecer los posibles riesgos en caso de su incumplimiento.
✓ Realizar la identificación de sus riesgos de corrupción, gestión y de seguridad de la información, para la identificación y valoración de los activos, serán orientados por la persona encargada de la seguridad de la información de la institución.
✓ En caso de materializarse un riesgo entregar al proceso de Direccionamiento estratégico un reporte de las causas que dieron origen a su materialización del riesgo y al incumplimiento de los objetivos y metas, a través del análisis de indicadores asociados.
✓ Realizar un Plan de mejora para los riesgos materializados con el fin de tomar medidas oportunas, el cual se radicará ante la oficina de Control Interno.
✓ Cuatrimestralmente, entregar al proceso de Direccionamiento Estratégico para su respectivo monitoreo, las evidencias que soporten el seguimiento y monitoreo de los controles y sus respectivas actividades con una semana de anterioridad al corte.

Segunda línea de defensa (Proceso de Direccionamiento Estratégico):

- ✓ Cuatrimestralmente, revisar la definición y articulación de los objetivos institucionales con los de cada proceso, junto con sus indicadores asociados.
- ✓ Cuatrimestralmente, evaluar y revisar el diseño de los controles para mitigar el riesgo entregados por los líderes de proceso.
- ✓ Realizar las recomendaciones necesarias a los controles.
- ✓ El proceso de Direccionamiento Estratégico, una vez reciba la información de los mapas, dispondrá de 5 días hábiles después de cada corte para la revisión tanto de los mapas como de las evidencias cargadas e informará a la Oficina de Control Interno.
- ✓ Hacer la consolidación de los riesgos en todos los niveles y reportarlo hacia la alta dirección.
- ✓ Publicar el Mapa de Riesgos en la página web institucional al 31 de enero de cada año.

Tercera línea defensa (Control Interno):

- ✓ Revisar cuatrimestralmente la ejecución de los controles establecidos por los líderes de proceso (riesgo inherente).
- ✓ Una vez reciba la información de los mapas por parte de Direccionamiento Estratégico, dispondrá de 5 días hábiles para realizar seguimiento y verificar la efectividad de los controles, así como, su respectiva publicación.
- ✓ Hacer un seguimiento cuatrimestralmente de las actividades de los controles (riesgo residual) y la coherencia de la calificación del impacto y probabilidad de los riesgos y dar las recomendaciones pertinentes.
- ✓ Publicar en la página web institucional el seguimiento realizado mediante un informe, a los diez primeros días hábiles posteriores al seguimiento.
- ✓ Revisar las evidencias entregadas por los líderes de proceso la cual debe ser coherente y que hayan entregado de manera oportuna.
- ✓ Realizar seguimiento y control de los Planes de mejora, entregados por los líderes de proceso en caso de materializarse el riesgo, el informe será entregado ante el comité de coordinación de Control Interno.
- ✓ Reportar a la Alta Dirección la ocurrencia de los riesgos de corrupción.

4. COMPROMISO FRENTE A LA POLÍTICA

El Instituto Superior de Educación Rural ISER de Pamplona, se compromete a gestionar los riesgos de corrupción, gestión y de seguridad de la información, monitorearlos y hacer seguimiento en forma cuatrimestral, identificando y administrando los eventos potenciales que pueden afectar los objetivos y los procesos del Instituto.

METODOLOGÍA:

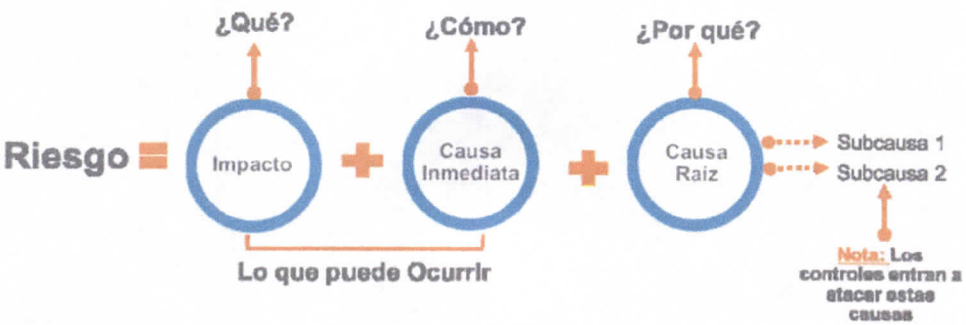
El proceso de Direccionamiento Estratégico se encargará de realizar la metodología que permita identificar, analizar, valorar y administrar los riesgos de gestión, de corrupción y de seguridad de la información, que se puedan presentar en el normal desarrollo de las actividades y que afecten el cumplimiento a la misión institucional y el logro de los objetivos estratégicos; esta metodología también establecerá el tratamiento, manejo, monitoreo y seguimiento conforme a la guía suministrada por el Departamento Administrativo de la Función Pública – DAFP. En esta metodología se incluirán los lineamientos para que cada proceso inicie su análisis y diligenciamiento correcto, en la que se incluyen los siguientes puntos:

1. IDENTIFICACIÓN DEL RIESGO:

Riesgos de gestión:

Cada líder de proceso y su equipo de trabajo debe identificar las actividades en las que se obtenga evidencia o indicios de ocurrencia de riesgos que afecten el cumplimiento de los objetivos de proceso y estratégicos, así como la consecuencia económica y/o reputacional.

Los líderes de proceso con su equipo de trabajo realizan la descripción de sus riesgos la cual debe contener los detalles necesarios para la comprensión de terceras personas, la redacción inicia con la frase PROBABILIDAD DE, seguido de los siguientes puntos de la gráfica:



Fuente: Guía para la administración del riesgo y el diseño de controles en las entidades públicas. Versión 5.
Función pública diciembre de 2020.

Los riesgos se clasificarán teniendo en cuenta las siguientes categorías:

CLASIFICACIÓN DE RIESGOS	
Ejecución y administración de procesos	Pérdidas derivadas de errores en la ejecución y administración de procesos
Fraude externo	Pérdida derivada de actos de fraude por personas ajenas a la organización (no participa personal de la entidad).
Fraude interno	Pérdida debido a actos de fraude, actuaciones irregulares, comisión de hechos delictivos abuso de confianza, apropiación indebida, incumplimiento de regulaciones legales o internàs de la entidad en las cuales está involucrado por lo menos 1 participante interno de la organización, son realizadas de forma intencional y/o con ánimo de lucro para sí mismo o para terceros.
Fallas tecnológicas	Errores en hardware, software, telecomunicaciones, interrupción de servicios básicos.
Relaciones laborales	Pérdidas que surgen de acciones contrarias a las leyes o acuerdos de empleo, salud o seguridad, del pago de demandas por daños personales o de discriminación.
Usuarios, productos y prácticas	Fallas negligentes o involuntarias de las obligaciones frente a los usuarios y que impiden satisfacer una obligación profesional frente a éstos.
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.

Esta clasificación se tiene en cuenta en relación con los factores de riesgo, de acuerdo a la naturaleza de la institución.

Riesgos de corrupción:

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

Las preguntas clave para la identificación del riesgo son

- ✓ ¿Qué puede suceder?
- ✓ ¿Cómo puede suceder?
- ✓ ¿Cuándo puede suceder?
- ✓ ¿Qué consecuencias tendría su materialización?

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

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

Fuente: Guía para la administración del riesgo y el diseño de controles en las entidades públicas. Versión 5.
Función pública diciembre de 2020.

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

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

El líder de proceso, como primer paso para la identificación de riesgos de seguridad de la información debe identificar los activos de información del proceso.

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

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

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.

Amenazas: Las amenazas pueden ser de origen natural o humano y podrían ser accidentales o deliberadas.

Vulnerabilidades: Estas se encuentran asociadas a la amenaza identificada.

Se pueden identificar vulnerabilidades en las siguientes áreas:

- ✓ Organización.
- ✓ Procesos y procedimientos.
- ✓ Rutinas de gestión.
- ✓ Personal
- ✓ Ambiente físico
- ✓ Configuración del sistema de información.
- ✓ Hardware, software y equipos de comunicaciones.
- ✓ Dependencia de partes externas.

Formato de descripción del riesgo de seguridad de la información:

El líder de proceso diligenciará el respectivo formato para la descripción teniendo en cuenta el suministro de la información anterior.

		INCLUYE ACTIVO-AMENAZA-VULNERABILIDADES				
RIESGO	ACTIVO	DESCRIPCIÓN DELRIESGO	AMENAZA	TIPO	CAUSAS/ VULNERABILIDADES	CONSECUENCIAS

Fuente: Guía para la administración del riesgo y el diseño de controles en las entidades públicas.
Función pública octubre de 2018.

2. VALORACIÓN DEL RIESGO:

Establece la probabilidad de ocurrencia del riesgo y el nivel de impacto con el fin de estimar la zona del riesgo inicial (RIESGO INHERENTE).

Riesgos de gestión y seguridad de la información:

Probabilidad: El líder de proceso analiza el número de veces que se pasa por el punto de riesgo en la vigencia (Exposición del riesgo), una vez tenga los datos de la frecuencia y de acuerdo a la siguiente tabla determina el porcentaje 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 las entidades públicas. Versión 5.
Función pública diciembre de 2020.

Impacto: Según el impacto económico y/o reputacional, el líder de proceso define el nivel de impacto de acuerdo a la siguiente tabla:

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

Fuente: Guía para la administración del riesgo y el diseño de controles en las entidades públicas. Versión 5.
Función pública diciembre de 2020.

En caso que se presenten ambos impactos para un riesgo, con diferentes niveles, se debe tomar el de nivel más alto.

La probabilidad y el impacto de los riesgos de seguridad de la información se determinan con base en la amenaza, no en las vulnerabilidades.

Riesgos de corrupción:

Para los riesgos de corrupción, la tabla de probabilidad es la misma que se utiliza para los riesgos de gestión, es decir la determinación de la probabilidad (posibilidad de ocurrencia del riesgo) se debe llevar a cabo de acuerdo con lo establecido en la parte inicial de la política.

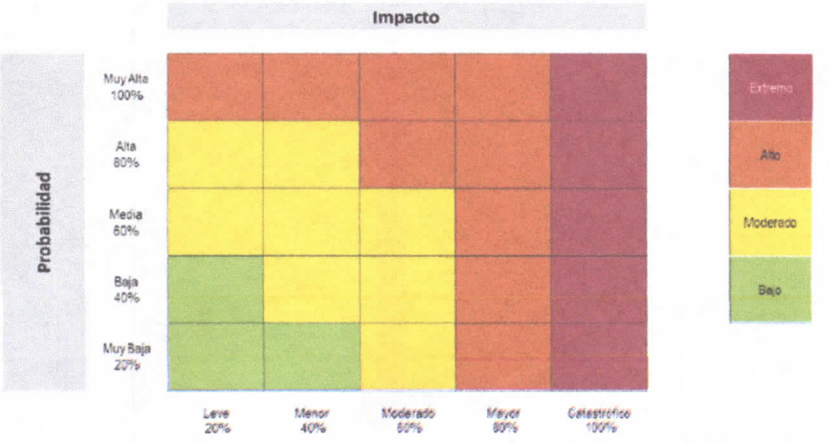
Para la determinación del impacto frente a posibles materializaciones de riesgos de corrupción, se analizarán únicamente los siguientes ***niveles i) moderado, ii) mayor, y iii) catastrófico,*** dado que estos riesgos siempre serán significativos, en tal sentido, no aplican los niveles de impacto insignificante y menor, que sí aplican para las demás tipologías de riesgos.

Ahora bien, para establecer estos niveles de impacto se deberán aplicar una serie de preguntas contenidas en la Guía para la Administración del Riesgo Versión 5 del 2020.

3. EVALUACIÓN DE RIESGO:

Riesgos de gestión y seguridad de la información:

Una vez se realiza el análisis de la probabilidad e impacto, el líder de proceso determina la zona de riesgo inicial (Riesgo Inherente), ubicando los resultados en la siguiente matriz:

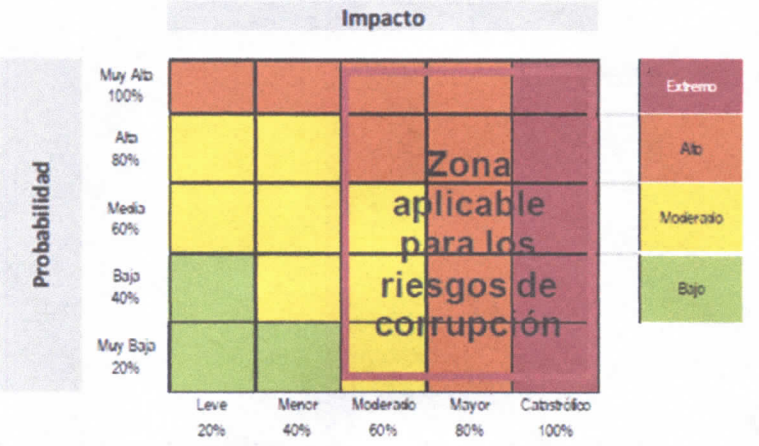


Fuente: Guía para la administración del riesgo y el diseño de controles en las entidades públicas. Versión 5.
Función pública diciembre de 2020.

El punto donde se cruza los datos de la probabilidad y el impacto será la severidad del riesgo, que se puede clasificar en Extremo, Alto, Moderado o Bajo, de acuerdo a la gráfica anterior.

Riesgos de corrupción:

El líder de proceso define el nivel de severidad para el riesgo, teniendo en cuenta el ajuste frente a los niveles de impacto, delimitado como se muestra a continuación:



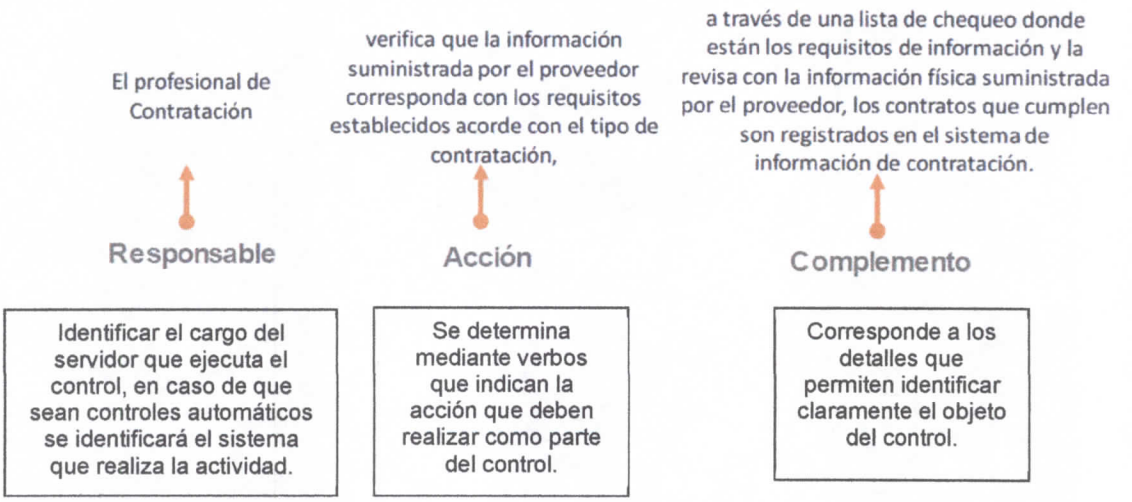
Fuente: Guía para la administración del riesgo y el diseño de controles en las entidades públicas. Versión 5.
Función pública diciembre de 2020.

4. CONTROLES:

Riesgos de gestión y de corrupción:

Los líderes de proceso junto con su equipo de trabajo, se encargan del diseño, implementación, ejecución y monitoreo de sus controles.

Para la correcta redacción de los controles deben tener en cuenta la siguiente estructura:



Fuente: Guía para la administración del riesgo y el diseño de controles en las entidades públicas. Versión 5.
Función pública diciembre de 2020 y modificada por la Institución

EL ANÁLISIS Y LA EVALUACIÓN DE LOS CONTROLES-ATRIBUTOS:

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

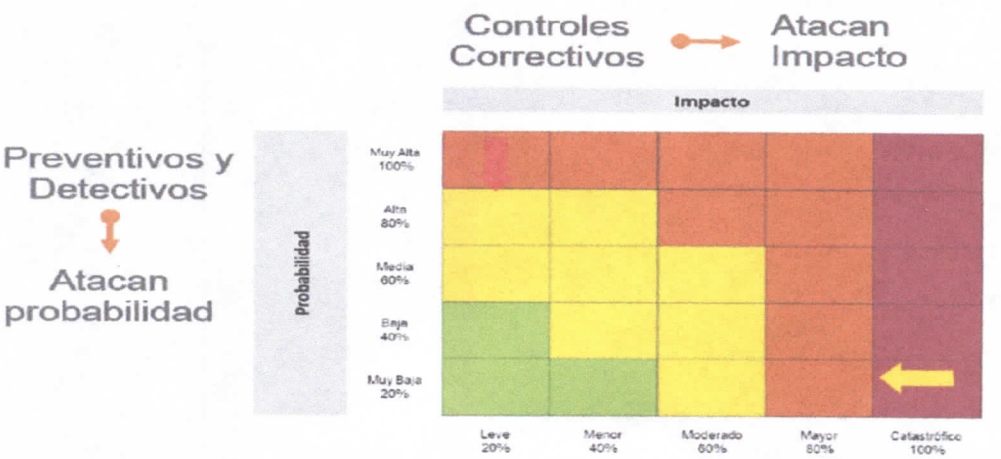
Características		Descripción		Peso
Atributos de eficiencia	Tipo	Preventivo	Va hacia las causas del riesgo, aseguran el resultado final esperado.	25%
		Detectivo	Detecta que algo ocurre y devuelve el proceso a los controles preventivos. Se	15%

			pueden generar reprocesos.	
		Correctivo	Dado que permiten reducir el impacto de la materialización del riesgo, tienen un costo en su implementación.	10%
	Implementación	Automático	Son actividades de procesamiento o validación de información que se ejecutan por un sistema y/o aplicativo de manera automática sin la intervención de personas para su realización.	25%
		Manual	Controles que son ejecutados por una persona, tiene implícito el error humano.	15%
Atributos informativos	Documentación	Documentado	Controles que están documentados en el proceso, ya sea en manuales, procedimientos, flujogramas o cualquier otro documento propio del proceso.	-
		Sin documentar	Identifica a los controles que pese a que se ejecutan en el proceso no se encuentran documentados en ningún documento propio del proceso.	-
	Frecuencia	Continua	El control se aplica siempre que se realiza la actividad que conlleva el riesgo.	-
		Aleatoria	El control se aplica aleatoriamente a la actividad que conlleva el riesgo	-
	Evidencia	Con registro	El control deja un registro permite evidencia la ejecución del control.	-
		Sin registro	El control no deja registro de la ejecución del control.	-

Fuente: Tabla tomada de la Guía para la administración del riesgo y el diseño de controles en las entidades públicas. Versión 5.
Función pública diciembre de 2020.

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.

Los controles permiten dar el movimiento en la matriz de calor en el eje de probabilidad y en el eje de impacto de acuerdo a su tipo, tal y como se muestra a continuación:



Fuente: Guía para la administración del riesgo y el diseño de controles en las entidades públicas. Versión 5.
Función pública diciembre de 2020.

Con la aplicación efectiva de los controles se determina un nuevo nivel de riesgo, 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 ubicar el riesgo después de los controles el líder de proceso deberá realizar la siguiente ecuación por cada uno de los controles, teniendo en cuenta que éstos mitigan de forma acumulativa:

% de (probabilidad o impacto) inherente * % valoración control 1 = % de mitigación parcial control 1

Seguido

Al % de (probabilidad o impacto) le resta (-) el % de mitigación parcial = % de mitigación final del control 1

Si tiene más de un control debe aplicar la siguiente fórmula y así en adelante con los demás controles:

% de mitigación final del control 1 * % valoración control 2 = % de mitigación parcial control 2

Seguido

Al % de mitigación final del control 1 le resta (-) el % de mitigación parcial del control 2 = % de mitigación final del control 2 (dependiendo de los controles este será el valor de su (probabilidad o impacto) residual)

Si no se tiene control para mitigar la probabilidad (detectivos y preventivos) o el impacto (Correctivos), se deja el mismo porcentaje calculado inicialmente.

De acuerdo a los porcentajes de impacto y probabilidad residuales, se ubicará el riesgo determinando la nueva zona en la matriz de calor.

Riesgos de seguridad de la información:

Para el tratamiento de estos riesgos se emplean los controles del Anexo A de la norma NTC: ISO/IEC 27001, estructurados de la siguiente forma:

Tabla 1. Estructura de controles

Política general			
Núm.	Nombre	Seleccionado / Excepción	Descripción / Justificación
	Nombre	Control	
	...		

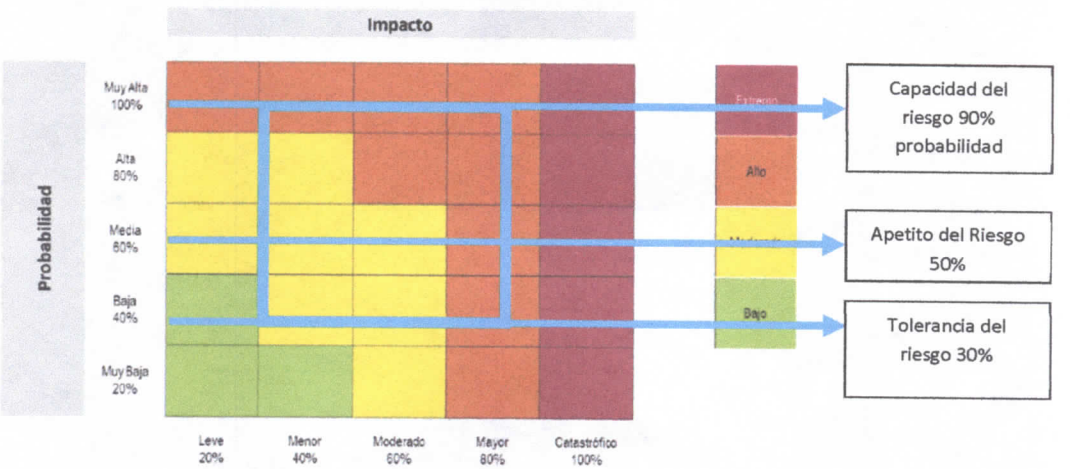
Fuente: Instrumento de Evaluación MSPI, Guía 8-Controles de Seguridad de la Información

5. NIVELES DE ACEPTACIÓN DEL RIESGO O TOLERANCIA AL RIESGO:

Establece "los niveles aceptables de desviación relativa a la consecución de los objetivos" (NTC GTC 137 Numeral 3.7.16), los mismos están asociados a la estrategia de la entidad y pueden considerarse para cada uno de los procesos.

- ✓ Los riesgos de corrupción son inaceptables.
- ✓ La aceptación del riesgo puede ocurrir sin tratamiento del riesgo.
- ✓ Los riesgos aceptados están sujetos a monitoreo

El apetito del riesgo se define a partir del análisis del nivel del riesgo el cual se realiza una vez se han identificado los controles para conocer el nivel de riesgo residual, siendo este nivel resultado de la evaluación de la probabilidad con el impacto, en la institución se fija el apetito del riesgo (valor máximo del nivel que está dispuesta a asumir para conseguir los objetivos institucionales), luego se define hasta qué limite la entidad está dispuesta a asumir los riesgos en el normal desarrollo de sus actividades (Capacidad del riesgo) y por último analizamos los niveles mínimos de exposición al que estaríamos dispuestos a llevar los riesgos (Tolerancia al riesgo), estos valores están representados en la siguiente gráfica:

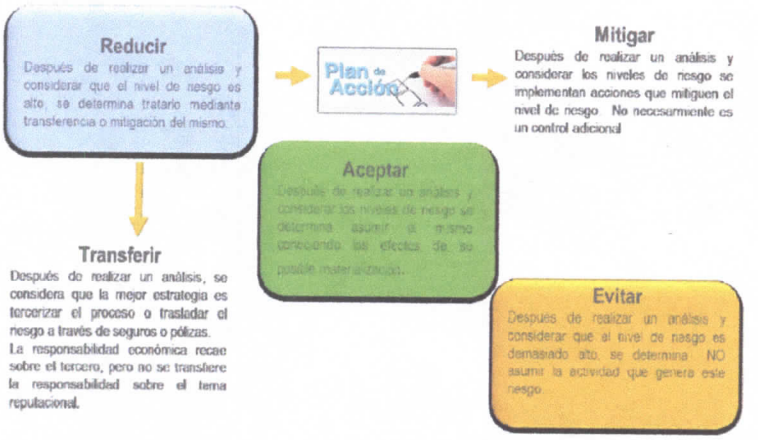


Fuente: Guía para la administración del riesgo y el diseño de controles en las entidades públicas. Versión 5.
Función pública diciembre de 2020.

Como se observa el apetito del riesgo deseado para el cumplimiento de los objetivos institucionales en condiciones normales para la entidad, se encuentra en una zona media de 50% de probabilidad y en un intervalo de impacto entre leve 30% y menor al 90%.

6. TRATAMIENTO DEL RIESGO

De acuerdo al nivel del riesgo cada líder de proceso determina que estrategia va a usar para combatir el riesgo, ya sea aceptar, reducir o evitar. Dependiendo de su relación con la necesidad se define si se debe realizar planes de mejora, como se muestra a continuación:



Fuente: Guía para la administración del riesgo y el diseño de controles en las entidades públicas. Versión 5. Función pública diciembre de 2020.

En caso de materialización:

- **Riesgos de Gestión y Seguridad de la Información (Zona Extrema, Alta y Moderada)**

Cada línea de defensa debe responder ante la materialización de los riesgos teniendo en cuenta las siguientes acciones:

Líder de proceso:

- ✓ Proceder de manera inmediata a aplicar el plan de contingencia o de tratamiento de incidentes de seguridad de la información que permita la continuidad del servicio o el restablecimiento del mismo (si es el caso), documentar en el Plan de mejoramiento.
- ✓ Iniciar el análisis de causas y determinar acciones preventivas y de mejora, documentar en el Plan de Mejoramiento Institucional y replantear los riesgos del proceso.
- ✓ Analizar y actualizar el mapa de riesgos.
- ✓ Informar al Proceso de Direccionamiento Estratégico sobre el hallazgo y las acciones tomadas.

Oficina de Control Interno:

- ✓ Informar al líder del proceso sobre el hecho encontrado.
- ✓ Informar a la segunda línea de defensa con el fin de facilitar el inicio de las acciones correspondientes con el líder del proceso, para revisar el mapa de riesgos.
- ✓ Acompañar al líder del proceso en la revisión, análisis y toma de acciones correspondientes para resolver el hecho.
- ✓ Verificar que se tomaron las acciones y se actualizó el mapa de riesgos correspondiente.

- **Riesgos de Gestión y Seguridad de la Información (Zona Baja)**

Líder de proceso:

✓ Establecer acciones correctivas al interior de cada proceso, a cargo del líder respectivo y verificar la calificación y ubicación del riesgo para su inclusión en el mapa de riesgos.

Oficina de Control Interno:

✓ Informar al líder del proceso sobre el hecho.
✓ Informar a la segunda línea de defensa con el fin facilitar el inicio de las acciones correspondientes con el líder del proceso, para revisar el mapa de riesgos.
✓ Acompañar al líder del proceso en la revisión, análisis y toma de acciones correspondientes para resolver el hecho.
✓ Verificar que se tomaron las acciones y se actualizó el mapa de riesgos correspondiente.

- **Riesgos de Corrupción**

Líder de proceso:

✓ Informar al Proceso de Direccionamiento Estratégico sobre el hecho encontrado.
✓ Una vez surtido el conducto regular establecido por la entidad y dependiendo del alcance (normatividad asociada al hecho de corrupción materializado), tramitar la denuncia ante la instancia de control correspondiente.
✓ Identificar las acciones correctivas necesarias y documentarlas en el Plan de mejoramiento.
✓ Efectuar el análisis de causas y determinar acciones preventivas y de mejora.
✓ Actualizar el mapa de riesgos.

Oficina de Control Interno:

✓ Informar al Líder del proceso, quien analizará la situación y definirá las acciones a que haya lugar.
✓ Una vez surtido el conducto regular establecido por la entidad y dependiendo del alcance (normatividad asociada al hecho de corrupción materializado), realizar la denuncia ante la instancia de control correspondiente.
✓ Informar a la segunda línea de defensa con el fin de facilitar el inicio de las acciones correspondientes con el líder del proceso, para revisar el mapa de riesgos.

7. MONITOREO Y REVISIÓN:

Los funcionarios y contratistas de la entidad deben conocer el mapa de riesgos de corrupción antes de su publicación. Para lograr este propósito el proceso de

Direccionamiento Estratégico, diseñará y pondrá en marcha las actividades o mecanismos necesarios para que los funcionarios y contratistas conozcan, debatan y formulen sus apreciaciones y propuestas sobre el proyecto del mapa de riesgos de corrupción, el cual se elabora con una periodicidad anual y debe hacer parte integral del Plan Anticorrupción y de Atención al Ciudadano conforme al Componente 1. Gestión del Riesgo de Corrupción – Mapa de Riesgos de Corrupción.

En cuanto al monitoreo y revisión, la periodicidad y responsabilidades se encuentran contenidas para cada línea de defensa mencionada en el numeral 3 de la presente política.

8. METODOLOGÍA PARA IDENTIFICACIÓN Y TRATAMIENTO DE LAS OPORTUNIDADES:

El tratamiento a las oportunidades inicia con su identificación dentro de la definición del contexto estratégico, aquí se hace referencia a las condiciones del entorno que pueden generar eventos positivos y los cuales originan oportunidades.

Los líderes de proceso se encargan de proponer las iniciativas estratégicas que desde cada proceso permita maximizar las oportunidades identificadas a medida que asegure el logro de los objetivos de calidad de la institución.

Las estrategias serán incluidas dentro de los Planes de Acción o Planes de Mejora del proceso con el fin de generar el reporte de los avances en el tiempo establecido en el momento en que se realicen los seguimientos por la segunda y tercera línea de defensa.

De acuerdo al plan en el que se establezcan las estrategias de las oportunidades, el proceso de Direccionamiento Estratégico y/o la oficina de Control Interno realizarán de forma cuatrimestral el seguimiento y monitoreo de las actividades ejecutadas por los líderes de proceso.

Los resultados del seguimiento serán reportados ante el Comité Institucional de Gestión y Desempeño y el Comité de Coordinación de Control Interno, a fin de facilitar la toma de decisiones frente a los avances obtenidos.

ARTÍCULO TERCERO. El proceso de Direccionamiento Estratégico con el apoyo del proceso de Gestión de la Comunicación, comunicará la Política para la Administración de Riesgos en todos los niveles de la institución, por medio de la página web institucional, comunicación por medio del correo institucional y mediante actividades de sensibilización a los procesos institucionales.

ARTÍCULO CUARTO. Esta política podrá contar con presupuesto, el cual será asignado en la medida que se requiera para el desarrollo de las actividades que operativicen la política. Los recursos financieros, tecnológicos, de infraestructura y otros, serán revisados y presentados en el presupuesto anual de la institución y deberán estar articulados al componente de Gestión del Riesgo de Corrupción – Mapa de Riesgos de Corrupción del Plan Anticorrupción y de Atención al Ciudadano que anualmente formula la institución.

ARTÍCULO QUINTO. El presente Acuerdo rige a partir de la fecha de su expedición y deroga todas las disposiciones que le sean contrarias.

PUBLÍQUESE, COMUNÍQUESE Y CÚMPLASE

Dado en Pamplona, a los treinta (30) del mes de Agosto del 2021

CLARA MARCELA ANGULO SANTANDER
El Presidente Delegada.

GLORIA CORONADO SEPULVEDA
Secretaria.

Proyectó:
Mónica Enith Salanueva Abril
Profesional Especializada Direccionamiento Estratégico

Revisó:

Janeth León Tarazona
Profesional Especializada Gestión Jurídica