



**ACUERDO 002 DE 2023
ENERO 27 DE 2023**

“POR EL CUAL SE APRUEBA LA POLÍTICA INSTITUCIONAL DE ADMINISTRACIÓN DEL RIESGO, DEL INSTITUTO NACIONAL DE FORMACIÓN TÉCNICA PROFESIONAL DE SAN ANDRÉS Y PROVIDENCIA -INFOTEP”

EL CONSEJO DIRECTIVO DEL INSTITUTO NACIONAL DE FORMACIÓN TÉCNICA PROFESIONAL DE SAN ANDRÉS Y PROVIDENCIA -INFOTEP- EN EJERCICIO DE SUS ATRIBUCIONES LEGALES,

CONSIDERANDO

Que, el Instituto Nacional de Formación Técnica Profesional (INFOTEP) es una entidad pública, adscrita al Ministerio de Educación Nacional, creado por el Decreto No. 176 del 26 de enero de 1980, sustituido por el 570 de marzo 4 de 1981 y reorganizado por el Decreto Ley No 758 de 1988 en un Establecimiento Público de Educación Superior, del orden nacional, reestructurado mediante los Decreto 1095 y 1096 del 2004 y 1570 y 1571 del 3 de octubre de 2016.

Que, el artículo 33 literal a) del Acuerdo 004 del 22 de febrero de 2019, señala que “son funciones del Consejo Directivo, aprobar a propuesta del Rector y Consejo Académico las políticas de la Institución, los planes y programas que, conforme a la Ley Orgánica de Planeación y la Ley Orgánica de Presupuesto, deben proponerse para su incorporación a los planes sectoriales y a través de estos, al Plan Nacional de Desarrollo.

Que, mediante el Decreto 1083 de 2015, Decreto único del Sector Función Pública, modificado por el Decreto 1499 de 2017, establece el Modelo Integrado de Planeación y Gestión - MIPG, como lo conocemos hoy con políticas de gestión y desempeño institucional para el correcto ejercicio de las funciones de las entidades del estado.

Que, basados en la Guía para la administración del riesgo y el diseño de controles en entidades públicas, se definen los criterios orientadores respecto al tratamiento de los riesgos de gestión a fin de mitigar sus efectos en la Institución y de esta manera poder manejarlos y controlarlos.

Que, basados en la Guía para la Gestión del Riesgo de Corrupción de la Secretaría de Transparencia de la Presidencia de la República se define la metodología para abordar los riesgos de corrupción de la institución . p

Que, el INFOTEP tiene el desafío de avanzar en el desarrollo de sus procesos académicos y administrativos, arraigar su identidad en el contexto de la insularidad, fortalecer su presencia en la región, implementar nuevas formas de producción y transferencia del conocimiento, incorporar las tecnologías de la información y la comunicación en los procesos educativos para lo cual requiere formular y desarrollar una propuesta institucional que afiance su liderazgo regional y la visibilidad nacional en los ámbitos político, económico y social.

Que, en consideración de lo anterior, el Consejo Directivo del Instituto Nacional de Formación Técnica Profesional INFOTEP,

ACUERDA:

ARTÍCULO PRIMERO: Aprobar la Política Institucional de Administración del Riesgo del Instituto Nacional de Formación Técnica Profesional de San Andrés y Providencia - INFOTEP, el cual forma parte integral de este Acuerdo.

ARTÍCULO SEGUNDO: Este Acuerdo rige a partir de su publicación y deroga todas las disposiciones que le sean contrarias.

PUBLIQUESE Y CUMPLASE

Dado en san Andrés Isla, a los veintisiete (27) días del mes de enero de dos mil veintitrés (2023)


MARIA FERNANDA POLANIA CORREA
Presidenta


MARLON MITCHELL H.
Secretario Técnico



POLÍTICA DE ADMINISTRACION DEL RIESGO

1. PRESENTACIÓN

El Modelo Integrado de Planeación y Gestión MIPG es un marco de referencia para dirigir, planear, ejecutar, hacer seguimiento, evaluar y controlar la gestión de las entidades y organismos públicos, con el fin de generar resultados que atiendan los planes de desarrollo y resuelvan las necesidades y problemas de los ciudadanos, con integridad y calidad en el servicio, según dispone el Decreto 1499 de 2017.

MIPG busca mejorar la capacidad del Estado para cumplirle a la ciudadanía, incrementando la confianza de la ciudadanía en sus entidades y en los servidores públicos, logrando mejores niveles de gobernabilidad y legitimidad del aparato público y generando resultados con valores a partir de una mejor coordinación interinstitucional, compromiso del servidor público, mayor presencia en el territorio y mejor aprovechamiento y difusión de información confiable y oportuna es una de los objetivos de la puesta en marcha del Modelo Integrado de Planeación y Gestión MIPG.

Para INFOTEP la administración de riesgos es una herramienta fundamental que permite asegurar el cumplimiento de su misión institucional y el desarrollo de sus actividades mediante el cumplimiento de los objetivos trazados dentro de los planes institucionales y estratégicos de la entidad.

Por lo anterior, basados en la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, se definen los criterios orientadores respecto al tratamiento de los riesgos de gestión, y mediante la Guía para la Gestión del Riesgo de Corrupción de la Secretaría de Transparencia de la Presidencia de la República se define la metodología para abordar los riesgos de corrupción.

2. INTRODUCCIÓN

A través de esta política, se busca definir la política y lineamientos institucionales a emprender, lo

que sin duda permitirá dirigir el accionar de INFOTEP hacia el uso eficiente de los recursos y la continuidad en la prestación de los servicios con calidad, los cuales se encuentran alineados con la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas para los riesgos de gestión y Guía para la Gestión del Riesgo de Corrupción de la Secretaría de Transparencia de la Presidencia de la República para los riesgos de corrupción.

3. JUSTIFICACIÓN

Teniendo en cuenta que los riesgos son posibilidades de ocurrencia de toda situación que pueda desviar el normal desarrollo de las actividades de los procesos e impidan el logro de los objetivos estratégicos para el cumplimiento de la misión institucional, INFOTEP ha fortalecido su Proceso Estratégico, a partir del Modelo Integrado de Planeación y Gestión – MIPG en su dimensión de Direccionamiento Estratégico, y en particular, la política de Planeación Institucional a través del análisis y estructuración de los elementos de control definidos en el Sistema Integral de Gestión

Mediante una adecuada administración de los riesgos, la Alta Dirección pretende alcanzar los mejores niveles de conocimiento respecto a la gestión de estos en la entidad, elevar la productividad y garantizar la eficiencia y la eficacia de los procesos organizacionales.

4. ANTECEDENTES

INFOTEP ha identificado los riesgos en cada uno de los procesos, los cuales son sujetos a seguimiento y evaluación por parte de la Oficina de Planeación (riesgos de gestión) y Control Interno (riesgos de corrupción).

Los elementos que fueron identificados y que son determinantes para la creación de esta política se relacionan con los factores externos, también denominados del entorno y factores de carácter interno. Entre los factores externos se destacan la normatividad, las reformas a la administración y los constantes recortes presupuestales que afectan la capacidad de

gestión de la institución. Entre los factores internos se destacan: El manejo de los recursos, la estructura organizacional, los controles existentes, los procesos y procedimientos, la disponibilidad presupuestal, la forma como se vinculan las personas a la institución, los intereses de los directivos, el nivel del talento humano, la motivación y los niveles salariales entre otros, que de alguna manera inciden en la materialización o no de situaciones que pueden generar riesgos para la institución.

La normatividad que permite la aplicación de esta política es la siguiente:

- Constitución Política de Colombia de 1991
- Ley 87 de 1993: Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del Estado y se dictan otras disposiciones.
- Ley 489 de 1998: Estatuto Básico de Organización y Funcionamiento de la Administración Pública
- Decreto 2145 de 1999: Por el cual se dictan normas sobre el Sistema Nacional de Control Interno de las Entidades y Organismos de la Administración Pública del orden nacional y territorial y se dictan otras disposiciones.
- Directiva presidencial 09 de 1999: Lineamientos para la implementación de la política de lucha contra la corrupción
- Decreto 2593 del 2000: Por el cual se modifica parcialmente el Decreto 2145 de noviembre 4 de 1999
- Decreto 1537 de 2001: Por el cual se reglamenta parcialmente la Ley 87 de 1993 en cuanto a elementos técnicos y administrativos que fortalezcan el sistema de control interno de las entidades y organismos del Estado.
- Decreto 1599 de 2005: Por el cual se adopta el Modelo Estándar de Control Interno para el Estado Colombiano y se presenta el anexo técnico del MECI 1000:2005. 1.3 Componentes de administración del riesgo.
- Decreto 943 de 2014: Por el cual se actualiza el Modelo Estándar de Control Interno (MECI).
- Decreto 4485 de 2009: Por el cual se adopta la actualización de la NTCGP a su versión

2009.

- Ley 1474 de 2011: Estatuto Anticorrupción
- Decreto 4637 de 2011: Crea la Secretaría de Transparencia en el Departamento Administrativo de la Presidencia de la República, quien establece lineamientos para la prevención de la corrupción.
- Decreto 1649 de 2014: Funciones de la Secretaría de Transparencia
- Ley 1712 de 2014: Ley de Transparencia y del Derecho al acceso a la información pública Nacional y se dictan otras disposiciones.
- Decreto 1081 de 2015: Señala como metodología para elaborar la estrategia de lucha contra la corrupción la contenida en el documento “Estrategias para la construcción del Plan Anticorrupción y de Atención al Ciudadano.”
- Decreto 1499 de 2018: por medio del cual se implementa el Modelo Integrado de Planeación y Gestión MIPG
- Ley 2195 de 2022: Por medio de la cual se adoptan medidas en materias de transparencia, prevención y lucha contra la corrupción y se dictan otras disposiciones.

5. OBJETIVO

Alcanzar un nivel aceptable de riesgos residuales en todos los procesos, a través de la gestión de acciones de control, con el fin de asegurar el cumplimiento de la misión institucional, los compromisos de gobierno, los objetivos estratégicos y de procesos vigentes.

6. POLÍTICA

Establecer el marco general para la administración de los riesgos en INFOTEP mediante la ejecución de un proceso metódico y continuo que contribuya al mejoramiento constante de las actividades y al cumplimiento de los objetivos de la Institución.

6.1 Metodología a utilizar

Se utilizará para riesgos de gestión o institucionales incluidos los de seguridad de la información la metodología vigente publicada por el Departamento Administrativo de la Función Pública DAFP para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas y/o la que modifique o sustituya. Para riesgos de corrupción la metodología adoptada es la establecida por la Secretaría de Transparencia de la Presidencia de la República.

6.2 Niveles de aceptación del riesgo o tolerancia al riesgo

Ningún riesgo de corrupción podrá ser aceptado

Los demás riesgos de gestión incluidos los de seguridad digital identificados en zona de riesgo **baja** se aceptarán, y se administrarán por medio de las actividades propias de los procesos o procedimientos asociados.

6.3 Lineamientos generales

El aspecto central para el desarrollo y la consolidación de la política de administración de riesgos, es la identificación y análisis del mapa de riesgos institucional y la formulación y actualización de la matriz de riesgos (matriz de calor y zonas de riesgo) con base en los siguientes criterios:

- Los riesgos siempre deben asociarse a los objetivos o estrategias definidas en el INFOTEP, objetivos de los procesos o proyectos. Un prerequisite indispensable para trabajar en la identificación de riesgos consiste en el entendimiento uniforme y completo de los objetivos y estrategias que se establezcan en la entidad, en el marco de su contexto estratégico.
- Los mapas de riesgos de gestión y corrupción, serán de conocimiento de la alta dirección, y su riesgo residual será el soporte para aprobación y/o modificación de la política de administración del riesgo.
- Los mapas de riesgos deben estar alineados con el Sistema Integrado de Gestión y con la planeación estratégica de la entidad.
- Se deben focalizar los riesgos residuales que queden ubicados en zona de riesgos extremos y altos con propósito de toma de decisiones en cuanto a su tratamiento.
- La opción de tratamiento o manejo para los riesgos residuales ubicados en zona de riesgo moderado, alto o extremos, no se podrán aceptar según lo establece la metodología, y a partir de este análisis deberán tener una propuesta o acción de tratamiento coherente que busquen gestionar el riesgo.

Nota: Aplica para riesgos de Gestión.

- Los riesgos residuales que queden ubicados en zona de riesgo bajo o muy bajo podrán llevar cualquiera de las opciones de manejo indicadas por el presente manual “aceptar, evitar, reducir”. Si se elige como tratamiento para el riesgo la opción de “aceptar el riesgo”, significará que para la vigencia no se generarán nuevos planes de acción para mitigar el riesgo. Sin embargo, el que se incluya esta opción no excluye al líder de proceso de la obligación de continuar aplicando los controles establecidos, y hacer el respectivo seguimiento tanto a los controles ya implementados como a la posible materialización del riesgo. Para riesgos de corrupción y/o soborno no se puede aceptar o asumir el riesgo.
- Para los riesgos de seguridad digital se debe implementar el anexo 4 ‘Modelo Nacional de Gestión de riesgo de seguridad de la Información en entidades públicas’ de la Guía para la administración de riesgos y el diseño de controles en entidades públicas, bajo el lineamiento del Ministerio de Tecnologías de la Información y Comunicaciones (MinTIC).

6.4 Lineamientos operativos para Mapas de Riesgos institucionales y de corrupción

- Los mapas de riesgos deberán ser aprobados por los líderes de los correspondientes procesos. Sin embargo, la oficina de Planeación, la Oficina de Control Interno y/o el Comité Institucional de Gestión y Desempeño, podrán solicitar se incluyan en el Mapa de Riesgos, aquellos riesgos potenciales que no hayan sido incluidos en los mapas de riesgos por procesos.
- Los mapas de riesgos deberán ser consolidados, publicados y socializados.
- Los mapas de riesgo deben como mínimo cubrir los riesgos asociados a las políticas MIPG
- La actualización de los mapas institucionales de riesgos de gestión, así como los mapas de riesgos de corrupción de demás modelos referenciales se realizarán de forma anual según lineamientos normativos, salvo que las necesidades del servicio requieran su actualización con otra periodicidad.
- La eliminación de cualquier riesgo deberá ser justificada y aprobada por el líder del proceso. Sin embargo, de presentarse justificaciones poco argumentadas, la oficina de Planeación, deberá pedir ampliación de la justificación, hasta tener evidencia de que dicha eliminación no acarreará perjuicios para la entidad, para lo cual se podrá solicitar concepto de otros líderes de procesos que puedan dirimir la decisión.
- Teniendo en cuenta la norma ISO 27001 de Seguridad de la Información, el área de gestión tecnológica deberá apoyar en la actualización de los riesgos de seguridad de la información a los que se puedan ver expuestos los diferentes procesos de la Entidad,
- Los riesgos de seguridad digital por su naturaleza e impacto se clasificarán como reservados. Es así como los riesgos identificados para INFOTEP en este sentido no deben ser públicos ya que esto expondría a la entidad y daría oportunidad de acceso a información reservada a terceros, situación que podría ser usada en su contra a través de posibles ataques cibernéticos, lo que generaría una vulneración de la plataforma informática y de los activos de información, en especial los denominados reservados y confidenciales.

Comunicación y Socialización de la Política de Gestión del Riesgo

La política de administración del riesgo en INFOTEP será comunicada a todos los niveles de la entidad, mediante alguno de los siguientes canales:

- Página WEB
- Correos electrónicos
- Ejercicios de Inducción y Re-Inducción dentro de las generalidades de MIPF
- Redes sociales

A través de estos canales se comunica o socializa contenidos relacionados con la gestión de los riesgos y aquellos orientados a generar conocimiento en los funcionarios y contratistas de la entidad.

6.5 Monitoreos

Los monitoreos les corresponden a la línea estratégica, primera y segunda línea de defensa. Se desarrollarán de la siguiente manera:

Línea Estratégica: el Comité de Coordinación de Control Interno realizará monitoreo cada semestre, para verificar el cumplimiento de la política de administración de riesgos.

Primera Línea de Defensa: Realiza monitoreo cuatrimestral a las acciones tendientes a controlar y gestionar los riesgos y enviará a la Oficina de Planeación los resultados de esos monitoreos cinco días antes de terminarse el cuatrimestre.

Segunda Línea de Defensa: Realizará monitoreo cuatrimestral a través de los informes que los líderes de procesos remitan, asegurando que los controles y los procesos de gestión de riesgos implementados por la primera línea de defensa, estén diseñados apropiadamente y funcionen como se pretende.

- **Seguimiento:** El seguimiento de los riesgos de corrupción le corresponde a la tercera línea de defensa, la oficina de control interno. Quien provee aseguramiento (evaluación) independiente y objetivo sobre la efectividad de los mis validando que la línea estratégica, la primer línea y segunda línea de defensa cumplan con sus responsabilidades en la gestión de riesgos para el logro en el cumplimiento de los objetivos institucionales y de proceso. La periodicidad de la

evaluación de los riesgos por parte de la Oficina de Control Interno, se definirá de acuerdo con los lineamientos generados por el Departamento Administrativo de la Función Pública DAFP.

El Jefe de Control Interno o quien haga sus veces, debe adelantar seguimiento a la gestión del riesgo, verificando la efectividad de los controles de la siguiente manera:

- Primer seguimiento: Con corte al 30 de abril
- Segundo seguimiento: Con corte al 31 de agosto
- Tercer seguimiento: Con corte al 31 de diciembre

El seguimiento adelantado por la Oficina de Control Interno se deberá publicar en la página web o en un lugar visible dentro de los diez (10) primeros días siguientes a la fecha de corte.

Los riesgos institucionales o de gestión se les realiza el seguimiento por parte de la oficina de Control Interno cada cuatro meses.

Si algún riesgo se llegara a materializar y esto es detectado por el líder del proceso se deben seguir los siguientes pasos:

1. Informa o reportar al Representante de la Alta Dirección para el MIPG.
2. De ser necesario, realizar la denuncia ante el ente de control respectivo
3. Iniciar las acciones correctivas necesarias.
4. Realizar el análisis de causas y determinar acciones de mejora.
5. Actualizar el mapa de riesgos.

Además de la evaluación de riesgos, la Oficina de Control Interno valorará el estado de la implementación, la efectividad de las medidas de administración, el diseño de los controles, junto con el nivel final de exposición al riesgo.

Si la oficina de Control Interno en los seguimientos establecidos evidencia que un riesgo de corrupción se materializó, debe seguir los siguientes pasos:

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.

2. Dependiendo del alcance (normatividad asociada al hecho de corrupción materializado), realizar la denuncia ante el ente de control respectivo.
3. Verificar que se tomaron las acciones y se actualizó el mapa de riesgos

6.6 Roles y Responsabilidades

Los roles y responsabilidades para la administración del riesgo por procesos, definidos en la entidad, son las siguientes:

Línea de Defensa	Responsable	Responsabilidad Frente al Riesgo
<p style="text-align: center;">Línea Estratégica</p>	<ul style="list-style-type: none"> – Alta Dirección – Comité de Coordinación de Control Interno – Comité Institucional de Gestión y Desempeño 	<p>Esta línea al ser una instancia decisoria dentro del sistema de Control Interno, su rol principal es analizar los riesgos y amenazas institucionales, que puedan afectar el cumplimiento de los planes estratégicos, así como definir el marco general para la gestión del riesgo (política de administración del riesgo) y el cumplimiento de los planes de la entidad. Los aspectos clave para el Sistema de Control Interno SCI a tener en cuenta por parte de la Línea Estratégica:</p> <ul style="list-style-type: none"> – Fortalecimiento del Comité Institucional de Coordinación de Control Interno incrementando su periodicidad para las reuniones. – Evaluación de la forma como funciona el Esquema de Líneas de Defensa, incluyendo la línea estratégica. – Definición de líneas de reporte (canales de comunicación) en temas clave para la toma de decisiones, atendiendo el Esquema de Líneas de Defensa. – Definición y evaluación de la Política de Administración del Riesgo. La evaluación debe considerar su aplicación en la entidad, cambios en el entorno que puedan definir ajustes, dificultades para su desarrollo, riesgos emergentes. – Evaluación de la política de gestión estratégica del Talento Humano (forma de provisión de los cargos, capacitación, código de Integridad, bienestar) – Define el marco general para la gestión del riesgo y el control; y supervisa su cumplimiento.
<p style="text-align: center;">Primera Línea de Defensa</p>	<ul style="list-style-type: none"> – Líderes de Procesos. 	<ul style="list-style-type: none"> – Esta línea está bajo la responsabilidad, principalmente, de los líderes de programas, procesos y proyectos y de sus equipos de trabajo (en general servidores públicos en todos los niveles de la entidad, su rol principal es el mantenimiento efectivo de controles internos, la ejecución de gestión de riesgos y controles en el día a día. Para ello, identifica, evalúa, controla y mitiga los riesgos a través del “Autocontrol”. – Los aspectos clave para el Sistema de Control Interno SCI a tener en cuenta por parte de la 1ª Línea: – El conocimiento y apropiación de las políticas, procedimientos, manuales, protocolos y otras herramientas que permitan tomar

		<p>acciones para el autocontrol en sus puestos de trabajo.</p> <ul style="list-style-type: none"> - La identificación de riesgos y el establecimiento de controles, así como su seguimiento, acorde con el diseño de dichos controles, evitando la materialización de los riesgos. - El seguimiento a los indicadores de gestión de los procesos e institucionales, según corresponda. - La formulación de planes de mejoramiento, su aplicación y seguimiento para resolver los hallazgos presentados - La coordinación con sus equipos de trabajo, de las acciones establecidas en la planeación institucional a fin de contar con información clave para el seguimiento o autoevaluación aplicada por parte de la 2ª línea de defensa.
Segunda Línea de Defensa	<p>Oficina de Planeación</p> <ul style="list-style-type: none"> - Líderes de proyectos - Supervisores 	<ul style="list-style-type: none"> - Acompañar, orientar y entrenar a los líderes de procesos en la identificación, análisis, valoración y evaluación del riesgo. - Supervisar en coordinación con los demás responsables de esta segunda línea de defensa, que la primera línea identifique, analice, valore, evalúe y realice el tratamiento de los riesgos, que se adopten los controles para la mitigación de los riesgos identificados y se apliquen las acciones pertinentes para reducir la probabilidad o impacto de los riesgos. - Monitorear los controles establecidos por la primera línea de defensa acorde con la información suministrada por los líderes de procesos. - Evaluar que la gestión de los riesgos este acorde 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 seleccionados para el tratamiento de los riesgos identificados. - Orientar y hacer seguimiento a las pruebas del plan de continuidad de negocio. - Identificar cambios en el apetito del riesgo en la entidad, especialmente en aquellos riesgos ubicados en zona baja y presentarlos para su aprobación del Comité de Coordinación de Control Interno - Actualizar, según se requiera, los escenarios de riesgo y la documentación asociada al plan de continuidad de negocio - bajo su responsabilidad.
Tercera Línea de Defensa	Oficina de Control Interno	<ul style="list-style-type: none"> - Esta línea está bajo la responsabilidad de la (el) jefe de control interno; desarrollaran su labor a través de los siguientes roles a saber: liderazgo estratégico, enfoque hacia la prevención, evaluación de la gestión del riesgo, relación con entes externos de control y el de evaluación y seguimiento - Los aspectos clave para el Sistema de Control Interno SCI a tener en cuenta por parte de la 3ª Línea: - A través de su rol de asesoría, orientación técnica y recomendaciones frente a la administración del riesgo en coordinación con la Secretaría de Planeación - Monitoreo a la exposición de la organización al riesgo y realizar recomendaciones con alcance preventivo. - Asesoría proactiva y estratégica a la Alta Dirección y los líderes de proceso, en materia de control interno y sobre las responsabilidades en materia de riesgos. - Formar a la alta dirección y a todos los niveles de la entidad sobre las responsabilidades en materia de riesgos. - Informar los hallazgos y proporcionar recomendaciones de forma

		independiente. – 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 – Recomendar mejoras a la política de operación para la administración del riesgo
--	--	---

6.7 Metodología para el tratamiento de riesgos

El tratamiento de riesgos, es la respuesta establecida por la línea estratégica para la mitigación de los diferentes riesgos, incluyendo los riesgos de corrupción. A la hora de evaluar las opciones existentes en materia de tratamiento del riesgo, y partiendo de lo que establezca la política de administración del riesgo, los líderes de los procesos tendrán en cuenta la importancia del riesgo, lo cual incluye el efecto que puede tener sobre la entidad, la probabilidad e impacto del riesgo, y la relación costo beneficio de las medidas de tratamiento. Pero en caso de que una respuesta ante el riesgo, derive en un riesgo residual que supere los niveles aceptables para los procesos, se deberá volver a analizar y revisar dicho tratamiento. En todos los casos para los riesgos de corrupción, la respuesta será evitar, compartir o reducir el riesgo

6.7.1 Riesgos de gestión o institucional y seguridad digital

Tipo de riesgo	Zona de riesgo	Nivel de aceptación
Riesgos de Gestión y seguridad digital	Muy baja o Baja	Se ACEPTA el riesgo y se administra por medio de las actividades propias del proceso o procedimiento asociado y se realiza en el reporte cuatrimestral de su desempeño.
	Moderada	Se establecen acciones de control preventivas que permitan REDUCIR la probabilidad de ocurrencia del riesgo, se hace monitoreo cuatrimestral y se registran sus avances en la matriz establecida para tal fin.
	Alta y Extrema	Se adoptan medidas para REDUCIR O COMPARTIR la probabilidad o el impacto del riesgo, o ambos; esto conlleva a la implementación de controles. Periodicidad cuatrimestral.

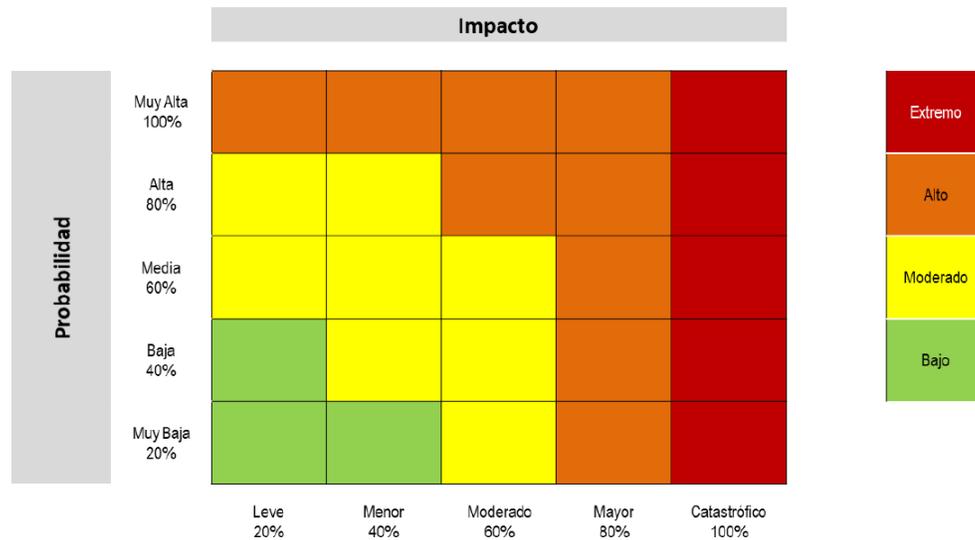
Para el caso de la probabilidad se utiliza la tabla de probabilidad (según la guía DAFP)

	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%

Se adopta la siguiente tabla con los criterios para calificar el impacto

ve 20%	Afectación menor a 200 SMLMV.	El riesgo afecta la imagen de algún área de la organización.
Menor 40%	Entre 201 y 1000 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 1001 y 5000 SMLMV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos.
Mayor 80%	Entre 5000 y 1000 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 10.000 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país.

Para poder identificar la zona de riesgo y los niveles de severidad, se utilizará el siguiente mapa de calor a través de la combinación de la probabilidad y el impacto determinados tanto para los riesgos inherentes como para los residuales.

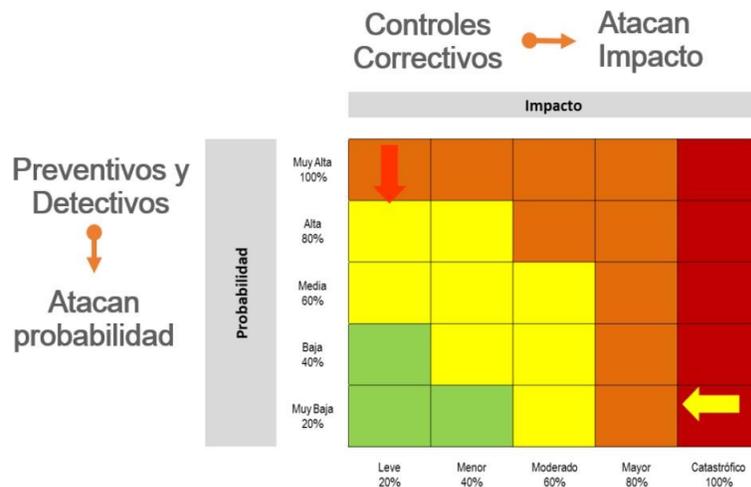


A continuación, se analizan los atributos para el diseño del control, teniendo en cuenta características relacionadas con la eficiencia y la formalización. En la siguiente tabla se puede observar la descripción y peso asociados a cada uno así.

Características		Descripción		
Atributos de eficiencia	Tipo	Preventivo	Va hacia las causas del riesgo, aseguran el resultado final esperado.	25%
		Detectivo	Detecta que algo ocurre y devuelve el proceso a los controles preventivos. Se pueden generar reprocesos.	15%
		Correctivo	Dado que permiten reducir el impacto de la materialización del riesgo, tienen un costo en su implementación.	10%
	Implementación	Automático	Son actividades de procesamiento o validación de información que se ejecutan por un sistema y/o aplicativo de manera automática sin la intervención de personas para su realización.	25%
		Manual	Controles que son ejecutados por una persona, tiene implícito el error humano.	15%
Atributos informativos	Documentación	Documentado	Controles que están documentados en el proceso, ya sea en manuales, procedimientos, flujogramas o cualquier otro 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.	-

Teniendo en cuenta que es a partir de los controles que se dará el movimiento, en la **siguiente** matriz de calor **se muestra** cuál es el movimiento en el eje de probabilidad y en el eje de impacto de acuerdo con los tipos de controles.

Ilustración 4 matriz de calor



Teniendo en cuenta que el riesgo residual es el resultado de aplicar la efectividad de los controles al riesgo inherente, es importante tener presente que los controles 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.

Así las cosas, el manejo de riesgos se realiza según la siguiente tabla:

Opción para el manejo del riesgo	Descripción
Evitar el riesgo	<p>Cuando los escenarios de riesgo identificado se consideran demasiado extremos se puede tomar una decisión para evitar el riesgo, mediante la cancelación de una actividad o un conjunto de actividades.</p> <p>Se abandonan las actividades que dan lugar al riesgo, es decir, no iniciar o no continuar con la actividad que lo provoca.</p>
Compartir el riesgo	<p>Cuando es muy difícil para la entidad reducir el riesgo a un nivel aceptable o se carece de conocimientos necesarios para gestionarlo, este puede ser compartido con otra parte interesada que pueda gestionarlo con más eficacia. Cabe señalar que normalmente no es posible transferir la responsabilidad del riesgo.</p> <p>Se reduce la probabilidad o el impacto del riesgo transfiriendo o compartiendo una parte de este.</p> <p>Los riesgos de corrupción se pueden compartir, pero no se puede transferir su responsabilidad.</p>

<p>Reducir el riesgo</p>	<p>El nivel de riesgo debería ser administrado mediante el establecimiento de controles, de modo que el riesgo residual se pueda reevaluar como algo aceptable para la entidad. Estos controles disminuyen normalmente la probabilidad y/o el impacto del riesgo.</p> <p>Deben seleccionarse controles apropiados y con una adecuada segregación de funciones, de manera que el tratamiento al riesgo adoptado logre la reducción prevista sobre este.</p> <p>Se adoptan medidas para reducir la probabilidad o el impacto del riesgo, o ambos; por lo general conlleva a la implementación de controles.</p>
<p>Aceptar el riesgo</p>	<p>No se adopta ninguna medida que afecte la probabilidad o el impacto del riesgo.</p> <p>Importante: Ningún riesgo de corrupción debe ser aceptado.</p>

6.7.2 Riesgos de corrupción

Teniendo en cuenta que el Gobierno Nacional viene impulsando y desarrollando diferentes políticas públicas con miras a disminuir los niveles de corrupción en todos los ámbitos, la Secretaría de Transparencia de la Presidencia de la República en cumplimiento del artículo 73 de la Ley 1474 de 2011 diseñó una metodología para que todas las entidades determinen su Plan Anticorrupción y de Atención al ciudadano, la cual contempla como uno de sus componentes el levantamiento de los mapas de riesgos asociados a posibles hechos de corrupción. Adicional a ello, recientemente se expidió la Ley 2195 de 2022, nueva ley Anticorrupción cuya metodología de implementación se encuentra en proceso de elaboración por lo que se seguirá adoptando la metodología de la Secretaría de Transparencia de la Presidencia de la República.

Tipo de riesgo	Zona de riesgo	Nivel de aceptación
Riesgos de Corrupción	Muy baja, baja o Moderada	Se establecen acciones de control preventivas que permitan REDUCIR la probabilidad de ocurrencia del riesgo. Periodicidad bimestral de monitoreo para evitar a toda costa su materialización por parte de los procesos.
	Alta y Extrema	Se adoptan medidas para: REDUCIR la probabilidad o el impacto del riesgo, o ambos; por lo general conlleva a la implementación de controles. EVITAR Se abandonan las actividades que dan lugar al riesgo, decidiendo no iniciar o no continuar con la actividad que causa el riesgo.
		TRANSFERIR O COMPARTIR una parte del riesgo para reducir la probabilidad o el impacto del mismo. Periodicidad bimestral de monitoreo para evitar a toda costa su materialización por parte de los procesos a cargo de los mismos

7. ALCANCE

Esta política involucra a todos los procesos, proyectos, productos de INFOTEP y a cualquier acción que sea ejecutada por parte de los funcionarios y contratistas durante el ejercicio de sus funciones y en representación de la institución.

8. APLICABILIDAD

La política aplica a todos los funcionarios y contratistas de INFOTEP de tal manera que su accionar reduzca y/o disminuya la ocurrencia de los riesgos asociados a sus funciones.

La responsabilidad de los servidores públicos y demás colaboradores es llevar a cabo las directrices planteadas en esta política. Es un compromiso y responsabilidad de todos, conocer la Política y es su deber cumplirla y respetarla para el desarrollo de cualquier actividad o consulta

La presente política será renovada cuando se presenten nuevas normativas y/o lineamientos establecidos por ley o la función pública o cuando la evaluación de los riesgos indique niveles extremos de los mismos de manera recurrente.

9. RESPONSABLE DE IMPLEMENTACIÓN

El área responsable de la implementación de esta política será de la oficina de control.

10. PLAN DE TRABAJO

Es necesario realizar seguimiento a las actividades para lograr la aplicación de esta política mediante lo siguiente:

ESTRATEGIA	UNIDAD DE MEDIDA	INDICADOR	RESPONSABLE	PERIODICIDAD
Diseñar y/o actualizar la política de Administración de Riesgo	Número	Política de administración de riesgos diseñada	Planeación	Anual o cuando se requiera una actualización
Socializar la Política de Administración de Riesgo	Número	Cantidad de espacios de socialización	Planeación	Dentro de los 15 días hábiles a la aprobación de la política
Elaboración, Monitoreo y seguimiento a matrices de riesgo	Número	Matriz de riesgos de gestión y seguridad digital elaborada, monitoreada y con seguimiento Matriz de riesgos de corrupción elaborada, monitoreada y con seguimiento	Planeación y Control Interno	Cuatrimestral

11. ARTICULACIÓN CON EL MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN (MIPG)

Esta política se articula con las políticas de: Planeación Institucional, Seguimiento y evaluación del desempeño institucional, Transparencia, acceso a la información pública y lucha contra la corrupción, Fortalecimiento organizacional y simplificación de procesos y Control interno del Modelo Integrado de Planeación y Gestión, en cumplimiento al Decreto 1499 de 2017.

12. RECURSOS

Para la implementación de esta política se tiene en cuenta el presupuesto anual de la institución el cual incluye los recursos de talento humano, tecnológicos y financieros.

13. RIESGOS

La no implementación de la Política de Administración de Riesgos puede conllevar a situaciones no conformes en los procesos de la entidad, reflejándose en procedimientos demorados, pocos eficientes y servicios de baja calidad dentro del accionar de la entidad.

Para mitigar este riesgo es necesario que todos los funcionarios de la entidad se apropien de la comprensión de la metodología expuesta en esta política la cual fue tomada de la Guía para la administración del riesgo y el diseño de controles en entidades públicas y la guía de la Secretaría de Transparencia de la Presidencia de la República.