



**INSTITUTO DEPARTAMENTAL DE DEPORTE Y RECREACIÓN DEL QUINDÍO
“INDEPORTES QUINDÍO”**

RESOLUCIÓN N° 412 DEL 21 DE DICIEMBRE DE 2023.

**Política de Administración de Riesgos y Direccionamiento
Estratégico Indeportes Quindío.**

“Por medio de la cual se actualiza las políticas de administración de riesgo y se deroga la resolución N° 056 del 22 de marzo de 2018 del Instituto Departamental de Deporte y Recreación del Quindío “Indeportes Quindío”.

Contenido

Introducción	3
Propósito del documento	3
Glosario	4
Política de administración de riesgos.....	6
Objetivo de la política de riesgos	7
Alcance.....	8
Niveles de aceptación del riesgo.....	8
Contexto Estratégico.....	8
Responsabilidades	16
Nivel de calificación de probabilidad para riesgos de proceso y seguridad digital	30
Nivel de calificación de probabilidad para riesgos de corrupción.....	30
Niveles de calificación de impacto	31
Criterios para la evaluación de impacto de pérdida de continuidad.....	33
Acciones ante los riesgos materializados.....	34
Acciones a seguir en caso de materialización de riesgos de corrupción	34
Estrategia de seguimiento al plan de acción	38
Anexos	39

Tabla de tablas

Tabla 1. Contexto Estratégico Función Pública.....	9
Tabla 2. Responsabilidades de las Líneas de Defensa.....	16
Tabla 3. Calificación de probabilidad para riesgos proceso y seguridad digital	30
Tabla 4. Calificación de probabilidad para riesgos de corrupción.....	30
Tabla 5. Calificación de impacto para riesgos de proceso y seguridad digital	31
Tabla 6. Calificación del Impacto para los riesgos de Corrupción	32
Tabla 7. Criterios para la evaluación de impacto de pérdida de continuidad	33
Tabla 8. Acciones de respuesta a riesgos.....	35
Tabla 9. Seguimiento al mapa de riesgos y controles	37
Tabla 10. Estrategia de seguimiento al plan de acción	38

“Indeportes Quindío se compromete a administrar y mantener niveles aceptables en los riesgos institucionales de gestión, corrupción y seguridad digital, mediante el cumplimiento de la metodología propia para su gestión y las acciones de control detectivas y preventivas oportunas que permitan i) evitar la materialización ii) corregir de manera inmediata las eventualidades presentadas y iii) mitigar las consecuencias ante posibles materializaciones en los diferentes ámbitos institucionales”

Introducción

La estructuración del presente documento para Indeportes Quindío está basada en la [guía para la administración del riesgo](#) vigente y el diseño de controles en entidades públicas y se establece para asegurar el cumplimiento de la misión institucional y los objetivos estratégicos y de proceso.

La política está compuesta por el objetivo, alcance, niveles de aceptación al riesgo, niveles para calificar el impacto, el tratamiento de riesgos, el seguimiento periódico según nivel de riesgo residual y responsabilidad de gestión para cada línea de defensa.

Propósito del documento

Establecer el marco general de actuación de todos los servidores públicos de la entidad para la adecuada gestión de los riesgos y los potenciales escenarios de pérdida de continuidad de negocio, mediante la identificación de acciones de control, respuestas oportunas y estrategias institucionales ante las situaciones que puedan afectar el cumplimiento de la misionalidad y el logro de objetivos institucionales, disminuyendo las potenciales consecuencias negativas, reduciendo las vulnerabilidades ante las amenazas internas y externas o mejorando las capacidades institucionales de respuesta a eventos identificados o inesperados que afecten al talento humano, la infraestructura tecnológica o los servicios esenciales de los que depende la Entidad.

Glosario

- **Activo:** en el contexto de seguridad digital son elementos tales como aplicaciones de la organización, servicios web, redes, Hardware, información física o digital, recurso humano, entre otros, que utiliza la organización para funcionar en el entorno digital.
- **Amenazas:** situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización.
- **Apetito del 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 del riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.
- **Causa:** todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.
- **Causa inmediata:** circunstancias bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo.
- **Causa raíz:** causa principal o básica, corresponde a las razones por la cuales se puede presentar el riesgo.
- **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.
- **CICCI:** Comité Institucional de Coordinación de Control Interno.
- **Confidencialidad:** propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados.
- **Contingencia:** posible evento futuro, condición o eventualidad.
- **Continuidad del negocio:** capacidad de una organización para continuar la entrega de productos o servicios a niveles aceptables después de una crisis.
- **Control:** medida que permite reducir o mitigar un riesgo.

- **Crisis:** ocurrencia o evento repentino, urgente, generalmente inesperado que requiere acción inmediata.
- **CIGD:** Comité Institucional de Gestión y Desempeño.
- **Disponibilidad:** propiedad de ser accesible y utilizable a demanda por una entidad.
- **Integridad:** propiedad de exactitud y completitud.
- **Mapa de riesgos:** documento que resume los resultados de las actividades de gestión de riesgos, incluye una representación gráfica en modo de mapa de calor de los resultados de la evaluación de riesgos.
- **MIPG:** Modelo Integrado de Planeación y Gestión.
- **OTIC:** Oficina de las Tecnologías de la Información y las Comunicaciones.
- **OAC:** Oficina Asesora de Comunicaciones.
- **OAP:** Oficina Asesora de Planeación.
- **Probabilidad:** se entiende la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. La probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año.
- **Restablecimiento:** capacidad de la Entidad para lograr una recuperación y mejora, cuando corresponda, de las operaciones, instalaciones o condiciones de vida una vez se supera la crisis.
- **Riesgo:** efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales. Los eventos potenciales hacen referencia a la posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos.
- **Riesgo de seguridad de la información:** posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

- **Riesgo de corrupción:** posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.
- **Riesgo inherente:** nivel de riesgo propio de la actividad. El resultado de combinar la probabilidad con el impacto nos permite determinar el nivel del riesgo inherente, dentro de unas escalas de severidad.
- **Riesgo residual:** el resultado de aplicar la efectividad de los controles al riesgo inherente.
- **SIGI:** Sistema Gestión Institucional, aplicativo propio para la gestión de planeación riesgos e indicadores.
- **TIC:** Tecnologías de la Información y las Comunicaciones.
- **Vulnerabilidad:** representan la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.

Política de administración de riesgos

La política de administración de riesgos del Departamento Administrativo de Indeportes Quindío, tiene un carácter estratégico y está fundamentada en el [modelo integrado de planeación y gestión](#), la [guía para la administración del riesgo](#) y el diseño de controles en entidades públicas, con un enfoque preventivo de evaluación permanente de la gestión y el control, el mejoramiento continuo y con la participación de todos los servidores de la entidad.

Aplica para todos los niveles, áreas y procesos de la Entidad e involucra el contexto, la identificación, valoración, tratamiento, monitoreo, revisión, comunicación, consulta y el análisis de los siguientes riesgos:

- Los riesgos de gestión de proceso que pueda afectar el cumplimiento de la misión y objetivos institucionales.

- Los riesgos de posibles actos de corrupción a través de la prevención de la ocurrencia de eventos en los que se use el poder para desviar la gestión de lo público hacia un beneficio privado.
- Los riesgos de seguridad de la información que puedan afectar la confidencialidad, integridad y disponibilidad de la información de los procesos de la entidad.
- Los riesgos de continuidad de negocio que impiden la prestación normal de los servicios institucionales debido a eventos calificados como crisis.

Indeportes Quindío determina que el módulo de riesgos del sistema de gestión institucional – SGI -, es la herramienta para identificar, valorar, evaluar y administrar los riesgos de gestión, de corrupción y de seguridad digital, para lo cual la oficina asesora de planeación identifica los requerimientos funcionales, revisa periódicamente su adecuado funcionamiento, cargue de información y dispone un manual de uso para el servicio de todos los procesos.

El periodo de revisión e identificación de los riesgos institucionales se debe realizar cada vigencia, atendiendo la metodología vigente, una vez se defina el plan de acción anual, asegurando la articulación de éstos con los compromisos de cada proceso.

Objetivo de la política de riesgos

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.

Alcance

Aplica a todos los procesos, proyectos, servicios y planes de la entidad, conforme a cada tipo y clasificación de riesgo, bajo la responsabilidad de los líderes de proceso y líneas de defensa.

Niveles de aceptación del riesgo

Acorde con los riesgos residuales aprobados por los líderes de procesos y socializados en el comité institucional de coordinación de control interno, se debe definir la periodicidad de seguimiento y estrategia de tratamiento a los riesgos residuales aceptados.

Indeportes Quindío determina que para los riesgos residuales de gestión y seguridad digital que se encuentren en zona de riesgo baja, está dispuesto a aceptar el riesgo y no se requiere la documentación de planes de acción, sin embargo, se deben monitorear conforme a la periodicidad establecida.

Para los riesgos de corrupción no hay aceptación del riesgo, siempre deben conducir a formular acciones de fortalecimiento.

Contexto Estratégico

Tabla 1. Contexto Estratégico

Contexto Estratégico Indeportes Quindío		
Contexto Externo	Económicos y Financieros	Recaudo del departamento con el impuesto del cigarrillo nacional y extranjero, IVA de telefonía celular, IVA cedido a licores, estampillas ProDesarrollo, esta política nos da la directriz de la administración optima de los recursos.
	Legal	Cambios legales y normativos aplicables a la entidad y a los procesos, plan de desarrollo y normatividad aplicable a los temas de Indeportes Quindío, Estándares internacionales.
	Político /Gobierno	Cambio de gobierno y administración con nuevos planes y proyectos de desarrollo, Objetivos de Desarrollo Sostenible, nuevos directivos en la Institución Indeportes Quindío.

	Sociales y culturales	Manifestaciones, complejidad en la movilidad. Epidemias o Pandemias (indisponibilidad de personal clave o imposibilidad de acceso a las instalaciones.), las emergencias epidemiológicas pueden permitir evaluar la capacidad de los planes de contingencia institucionales o la materialización de riesgos de no disponibilidad de personal clave. Despliegue territorial: seguridad de los servidores públicos, desorden público, conflicto de intereses, prevención corrupción. Pandemia: nuevos enfoques de trabajo virtual, protección de los servidores públicos.
	Tecnológicos	Interoperabilidad de los sistemas de información, plataformas tecnológicas, requisitos de MinTic, seguridad de la información, servidores internos de la Entidad, falta de compatibilidad con otros sistemas, falta de recursos para el fortalecimiento tecnológico.

Contexto Estratégico Indeportes Quindío		
	Ambientales:	Desastres naturales, contaminación. Epidemias o Pandemias (indisponibilidad de personal clave o imposibilidad de acceso a las instalaciones.), las emergencias epidemiológicas pueden permitir evaluar la capacidad de los planes de contingencia institucionales o la materialización de riesgos de no disponibilidad de personal clave.
	Comunicación Externa:	Herramientas virtuales, canales de información, acceso a la tecnología en territorio. Adopción de las herramientas de nube privada para ofimática, implementación de estrategias de continuidad de negocio ante eventos disruptivos de la infraestructura tecnología de la sede, obliga al mejoramiento de los esquemas de roles y privilegios de usuario y los mecanismos de gestión de alta y baja de cuentas de usuario.
	Evento Externo	Situaciones externas que afectan la entidad.

Contexto Interno	Financieros:	Recursos, necesidades por parte de las dependencias, plan adquisiciones, comunicación, apropiación de recursos, comunicación entre las dependencias intervinientes en el proceso presupuestal.
Contexto Estratégico Indeportes Quindío		
Contexto Interno	Talento Humano	Planta de personal, competencias del personal a partir de la implementación del Modelo Integrado de Planeación y Gestión MIPG, desarrollo de habilidades, motivación e involucramiento del personal, concurso de méritos para proveer los cargos en provisionalidad. La incorporación de jóvenes profesionales a la entidad facilita la implementación de estrategias de cambio organización en materia de nuevas herramientas tecnológicas. La incorporación de nuevo personal obliga al mejoramiento de la calidad de los manuales de procesos y procedimientos de forma que el personal nuevo conozca completamente sus roles y responsabilidades.
	Procesos	Apropiación Modelo Integrado de Planeación y Gestión MIPG, participación del personal en campañas de socialización, documentar y tomar decisiones. Adopción de herramientas de flujo de trabajo basadas en nube. Teletrabajo y computación en la nube permiten la verificación de planes de contingencia y continuidad y obliga a mejorar la especificación de roles y responsabilidades para acceso a las aplicaciones y servicios institucionales

Contexto Estratégico Indeportes Quindío		
	Tecnología	Herramientas y aplicativos internos, servidores internos de la Entidad (Intranet, SGI, Página Web) Adopción de la computación en nube privada o nube publica para labores cotidianas institucionales, Teletrabajo y computación en la nube permiten la verificación de planes de contingencia y continuidad. Obliga al mejorar la especificación de roles y responsabilidades para acceso a las aplicaciones y servicios institucionales Nuevos tipos de riesgos informático relacionados con la suplantación de identidad institucional
	Estratégicos:	Planificación institucional, comunicación y solicitud de información a las dependencias, solicitud de información múltiple, información institucional, funciones y competencia de las dependencias de Indeportes Quindío. La identificación de registros vitales como documentos, servicios y sistemas de información posibilitan la mejor identificación de riesgos, por el contrario, una inadecuada calificación de acceso a los activos de información puede provocar acceso no autorizado a datos personales e información clasificada o reservada.
	Comunicación interna:	Temas gestionados por parte de Indeportes Quindío, canales internos, entrega de información. Adopción de herramientas de flujo de trabajo basadas en nube. Teletrabajo y computación en la nube permiten la verificación de planes de contingencia y continuidad y obliga a mejorar la especificación de roles y responsabilidades para acceso a las aplicaciones y servicios institucionales
	Infraestructura	Eventos relacionados con la infraestructura física de la entidad

Contexto Estratégico Indeportes Quindío		
Contexto Interno del Proceso	Diseño del Proceso	Reingeniería de procesos, mesas de construcción participativa, procesos compartidos en diferentes dependencias, coordinación.
		Elementos de innovación propuestos por el PND Requerimientos de inclusión, equidad, criterios diferenciales Visibilizar gestión estadística y de información Aplicativos y herramientas que operan con lo descrito en los procesos Planes, proyectos y presupuestos articulados al SIPG Procedimientos y flujos descritos en los procesos Riesgos institucionales integrados a los procesos Interoperabilidad de herramientas internas y externas Rediseñar y apropiar el proceso de acción integral Ajustar el proceso de TIC a Gobierno y transformación digital Manejo institucional de contingencias y continuidad Visibilizar en el SIPG la Secretaria General en el SIPG todas las dependencias y procesos
	Interacciones con otros procesos	Responsabilidad, autoridad y funciones, trabajo en equipo entre los procesos, políticas de operación.
		Articulación de la gestión del conocimiento con DGC, OTIC, GGD y GGH
	Procedimientos asociados	Actualización, socialización, procedimientos entre procesos.
	Responsables del proceso	Responsabilidad compartida, coordinación de los procesos, control de la ejecución de los procesos.
	Comunicación entre los procesos	Mecanismos de articulación entre los procesos (reuniones, canales, mecanismos de seguimiento).
		Adopción de herramientas de flujo de trabajo basadas en nube. Teletrabajo y computación en la nube permiten la verificación de planes de contingencia y continuidad y obliga a mejorar la especificación de roles y responsabilidades para acceso a las aplicaciones y servicios institucionales

Contexto Estratégico Función Pública		
	Activos de Seguridad Digital del proceso	Procedimientos y estructura de matrices inventario de activos de información, Riesgos de Seguridad Digital Planes de contingencia en caso de incidentes de seguridad, la falta de entrenamiento o divulgación en materia de incidentes de seguridad puede generar afectaciones serias en cuanto a prestación y continuidad de servicios generando pérdida de confianza del grupo de valor.

Fuente: Oficina Asesora de Planeación

Responsabilidades

La responsabilidad está definida mediante las líneas de defensa y en la entidad se acogen según la siguiente tabla:

Tabla 2. Responsabilidades de las Líneas de Defensa

Líneas de Defensa	Responsable	Responsabilidad frente al riesgo
Línea Estratégica	Alta Dirección, Equipo Directivo, Comité Institucional de Gestión y Desempeño.	- Definir el marco general para la gestión del riesgo, la gestión de la continuidad del negocio y el control. - Asegurar la implementación y desarrollo de las políticas de gestión y desempeño institucional que permitan apalancar la gestión del riesgo en diferentes ámbitos institucionales. - Generar recomendaciones de mejora a la política de administración del riesgo para su análisis e inclusión.
	Comité institucional de coordinación de control interno	Aprobar la política de administración del riesgo previamente estructurada por parte de la oficina asesora de planeación, como segunda línea de defensa en la entidad; hacer seguimiento para su posible actualización.

Líneas de Defensa	Responsable	Responsabilidad frente al riesgo
		• Evaluar la eficacia de la política frente a la gestión del riesgo institucional. Se deberá hacer especial énfasis en la prevención y detección de fraude y mala conducta. • Monitorear los riesgos críticos identificados (aquellos definidos en los niveles de severidad Alto y Extremo, independientemente de su nivel de probabilidad), mediante el análisis de eventos o materializaciones u otra información aportada por las instancias de 2ª línea identificadas. • Analizar los riesgos, vulnerabilidades, amenazas y escenarios de pérdida de continuidad de negocio institucionales que pongan en peligro el cumplimiento de los objetivos estratégicos, planes institucionales, metas, compromisos de la entidad y capacidades para prestar servicios, a partir de la información aportada por las instancias de 2ª línea identificadas. • Garantizar el cumplimiento de los planes institucionales, estratégicos y sectoriales de la entidad.
Primera Línea	Líderes de Procesos. Gerentes Operativos de programas y proyectos de la entidad. Servidores en general.	El líder del proceso debe: • Promover al interior de su equipo de trabajo el concepto de “administración de riesgo”, iniciando por la socialización de la política, su metodología allí desplegada y el marco de referencia de Indeportes Quindío aprobado por la línea estratégica. • Identificar, valorar, evaluar y actualizar cuando se requiera, los riesgos que pueden afectar los objetivos, programas, proyectos y planes asociados a su proceso y realizar seguimiento al mapa de riesgo del proceso a cargo. • Delegar, por parte del líder del proceso, el (los) profesionales que se encargaran de la identificación, monitoreo, reporte y socialización de los riesgos.

Líneas de Defensa	Responsable	Responsabilidad frente al riesgo
		- Definir, adoptar, aplicar y hacer seguimiento a los controles para mitigar los riesgos identificados y proponer mejoras para su gestión. - Revisar el adecuado diseño y ejecución de los controles establecidos para la mitigación de los riesgos y su documentación se evidencie en los procedimientos de los procesos. - Revisar de acuerdo con su competencia y alcance la documentación del plan continuidad del negocio. - Reportar en el SGI los avances y evidencias de la gestión de los riesgos dentro de los plazos establecidos. - Realizar la medición y análisis a la gestión efectiva de los riesgos. - 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. - Revisar las acciones y planes de mejoramiento establecidos para cada uno de los riesgos materializados, con el fin de que se tomen medidas oportunas y eficaces. - En caso de materialización de un riesgo identificado, Informar a la oficina de planeación (segunda línea) y aplicar las acciones correctivas o de mejora necesarias. - En caso de la materialización de un riesgo no identificado, este debe ser gestionado en el aplicativo SGI y ser incluido en el mapa de riesgo institucional, con el acompañamiento de la Oficina Asesora de Planeación - Analizar los resultados del seguimiento y establecer acciones inmediatas ante cualquier desviación.

Líneas de Defensa	Responsable	Responsabilidad frente al riesgo
		• Evaluar con el equipo de trabajo la responsabilidad y resultados de la gestión del riesgo, así como las desviaciones según el nivel de aceptación del riesgo al interior de su dependencia y las acciones a seguir. • Comunicar al equipo de trabajo los resultados de la gestión del riesgo. • Asegurar que se documenten las acciones de corrección o prevención en el plan de mejoramiento. • Revisar y actualizar el mapa de riesgos con el acompañamiento de la OAP. Los servidores en general deben: • Participar en el diseño de los controles que tienen a cargo. • Ejecutar los controles a su cargo de la forma como están diseñados. • Informar a su superior jerárquico sobre riesgos materializados o posibles situaciones de afectación al proceso, a fin de incorporar las acciones a que haya lugar. • Proponer mejoras a los controles existentes. Gerente Operativo de programas y proyectos de la entidad debe: • Realizar la identificación de los riesgos del proyecto. • Monitorear los riesgos identificados y controles definidos por la primera línea de defensa acorde con la estructura de los temas a su cargo. • Orientar a la primera línea de defensa para que identifique, valore, evalúe y gestione los riesgos y escenarios de pérdida de continuidad de negocio en los temas de su competencia. • Supervisar la implementación de las acciones de mejora o la adopción de buenas prácticas

Líneas de Defensa	Responsable	Responsabilidad frente al riesgo
		de gestión del riesgo asociado a su responsabilidad.
Segunda Línea	Servidores Responsables de Monitoreo y Evaluación de Controles y Gestión del Riesgo, Jefes de Planeación, Supervisores o Interventores de Contrato o Proyectos y Coordinadores de Otros Sistemas.	- Asesorar a la línea estratégica en el análisis del contexto interno y externo, incluyendo su actualización, acorde con los cambios en el entorno, la definición de la política de riesgo, el establecimiento de los riesgos al proceso de Direccionamiento acorde con los procesos definidos en el Nivel Estratégico de Función Pública del esquema de procesos actual, o bien el que lo actualice o sustituya cuando existan cambios en dicho esquema de operación. - Identificar cambios en el entorno (interno o externo) que afecten el apetito del riesgo en la entidad para su análisis y se adelanten los ajustes que correspondan a este aparte dentro de la presente política. - Capacitar al grupo de trabajo de cada dependencia en la herramienta SGI para la gestión del riesgo con la asesoría de la Dirección de Gestión y Desempeño Institucional como líder de la política de control interno. - Revisar el adecuado diseño de los controles a través de la metodología aplicada en el sistema de gestión institucional para la mitigación de los riesgos que se han establecido por parte de la primera línea de defensa y realizar las recomendaciones y seguimiento para el fortalecimiento de estos. - Verificar que las acciones de control se diseñen conforme a los requerimientos de la metodología. - Revisar el perfil de riesgo inherente y residual por cada proceso y pronunciarse sobre cualquier riesgo que este por fuera del perfil de riesgo residual aceptado por la entidad.

Líneas de Defensa	Responsable	Responsabilidad frente al riesgo
		- Hacer seguimiento al plan de acción establecido para la mitigación de los riesgos de los procesos registrados en el SGI. - Revisar que el cargue de información en el SGI esté acorde con lo aprobado por el líder del proceso. - Consolidar el mapa de riesgos institucional, riesgos de mayor criticidad frente al logro de los objetivos y presentarlo para análisis y seguimiento. - Presentar al Comité Institucional de Coordinación de Control Interno-CICCI el resultado de la medición del nivel de eficacia de los controles para el tratamiento de los riesgos identificados en los procesos o proyectos. - Acompañar, orientar y entrenar a los líderes de procesos en la identificación, análisis, valoración y evaluación del riesgo. - Coordinar con los líderes de proceso el responsable de reporte de seguimiento a los riesgos, controles y planes de acción en el aplicativo SGI. - Informar a la primera línea de defensa la importancia de socializar los riesgos aprobados al interior de su proceso. - Comunicar a los líderes de proceso a través de los enlaces los resultados de la gestión del riesgo. - Consolidar el mapa de riesgos institucional a partir de la información reportada por cada uno de los procesos (mapa de riesgo del proceso) y generar un reporte ejecutivo que permita establecer alertas a la Línea Estratégica sobre retrasos, incumplimientos u otras fallas detectadas - Socializar y publicar el mapa de riesgos institucional. - Participar en los ejercicios de autoevaluación de la eficiencia, eficacia y efectividad de los

Líneas de Defensa	Responsable	Responsabilidad frente al riesgo
		controles seleccionados para el tratamiento de los riesgos identificados que se adelanten al interior de la entidad. • Revisar las acciones y planes de mejoramiento establecidos para cada uno de los riesgos materializados, con el fin de que se tomen medidas oportunas y eficaces para evitar en lo posible que se vuelvan a materializar y lograr el cumplimiento a los objetivos. • Informar a la primera línea de defensa correspondiente (líder del proceso) la materialización de un riesgo no identificado, el cual debe ser gestionado en el aplicativo SGI y ser incluido en el mapa de riesgo institucional. • 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.
Segunda Línea	Jefes de Planeación	• El Jefe de Planeación (o a quien delegue), mensualmente consolidará el avance sobre la planeación institucional de manera articulada con los temas asociados a los proyectos de inversión y otros requerimientos externos (Presidencia, DNP, Altas Consejerías), generando alertas en semáforo sobre retrasos o posibles incumplimientos; al tiempo articulará la información sobre eventos (materializaciones de riesgo) asociados a los mismos permitiendo el análisis integral de la gestión del riesgo. El reporte se analiza en el Comité de Coordinación de Control Interno para definir acciones de mejora o intervenciones

Líneas de Defensa	Responsable	Responsabilidad frente al riesgo
		necesarias, información que aporta el Jefe de Planeación como gestor del proceso de direccionamiento estratégico.
	Supervisores o Interventores de Contrato o Proyectos, Coordinadores	El Supervisor o Interventor de Contrato o Proyectos mensualmente, consolida los avances del Plan Anual de Adquisiciones, de acuerdo a cada modalidad de contratación, generando alertas en semáforo frente a retrasos o posibles incumplimientos en los planes, programas o proyectos a los cuales se encuentran asociados los contratos analizados. La fuente para el análisis se basa en los informes de supervisión o interventoría (según corresponda) de los contratos en ejecución. El reporte se analiza en el Comité de Coordinación de Control Interno para definir acciones de mejora o intervenciones necesarias, información que aporta la Secretaria General como líder del proceso de gestión de recursos
	Coordinador de Talento Humano	El coordinador de TH, bimestralmente consolidará el avance sobre PIC, Bienestar, Incentivos y temas de convivencia laboral, mediante un análisis de variables relacionadas con la ejecución de cada uno de estos mecanismos, que permita generar alertas en la ejecución de recursos. En el tema de convivencia generar información sobre quejas reiteradas de acoso laboral, conflictos internos que no ha sido posible resolver y aquellos que llegan a instancia disciplinaria. El reporte se analiza en el Comité de Coordinación de Control Interno para definir acciones de mejora o intervenciones necesarias, información que aporta la Secretaria General como líder del proceso de gestión del Talento Humano.

Líneas de Defensa	Responsable	Responsabilidad frente al riesgo
Segunda Línea	Responsables de Monitoreo y Evaluación de Controles y Gestión de riesgos	• Monitorear los riesgos identificados y controles definidos por la primera línea de defensa acorde con la estructura de los temas a su cargo. • Sugerir las acciones de mejora a que haya lugar posterior al análisis, valoración, evaluación o tratamiento del riesgo. • Supervisar la implementación de las acciones de mejora o la adopción de buenas prácticas de gestión del riesgo asociado a su responsabilidad. • Participar en las pruebas del plan de continuidad del negocio y en la implementación. • Comunicar al equipo de trabajo a su cargo la responsabilidad y resultados de la gestión del riesgo.

Líneas de Defensa	Responsable	Responsabilidad frente al riesgo
Tercera Línea	Oficina de Control Interno o Auditoría Interna de la Entidad	- Revisar los cambios en el "Direccionamiento estratégico" o en el entorno y cómo estos pueden generar nuevos riesgos o modificar los que ya se tienen identificados en cada uno de los procesos, con el fin de que se identifiquen y actualicen las matrices de riesgos por parte de los responsables. - 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.

Líneas de Defensa	Responsable	Responsabilidad frente al riesgo
		• Proporcionar aseguramiento objetivo en las áreas identificadas no cubiertas por la segunda línea de defensa. • Asesorar a la primera línea de defensa de forma coordinada con la Oficina de Planeación, en la identificación de los riesgos y diseño de controles. • Llevar a cabo el seguimiento a los riesgos y estrategia de continuidad negocio consolidados en los mapas de riesgos y plan de continuidad de conformidad con el Plan Anual de Auditoria y reportar los resultados al CICCI. • Realizar seguimiento a la implementación de mejoras sobre los lineamientos de continuidad del negocio. • Realizar seguimiento a la implementación de la estrategia de continuidad del negocio y a las pruebas efectuadas. • Recomendar mejoras a la política de operación para la administración del riesgo.

Fuente: Oficina Asesora de Planeación

Nivel de calificación de probabilidad para riesgos de proceso y seguridad digital

Tabla 3. Calificación de probabilidad para riesgos proceso y seguridad digital

Nivel	Probabilidad	Descripción
100%	Muy Alta	La actividad se realiza más de 1500 veces al año.
80%	Alta	La actividad se realiza entre 366 a 1500 veces al año.
60%	Media	La actividad se realiza entre 13 a 365 veces al año.
40%	Baja	La actividad se realiza entre 5 a 12 veces al año.
20%	Muy Baja	La actividad se realiza máximo 4 veces al año.

Fuente: Oficina Asesora de Planeación

Nivel de calificación de probabilidad para riesgos de corrupción

Tabla 4. Calificación de probabilidad para riesgos de corrupción

Nivel	Probabilidad	Probabilidad	Descripción
5	Casi seguro	Se espera que el evento ocurra en la mayoría de las circunstancias.	Más de 1 vez al año.
4	Probable	Es viable que el evento ocurra en la mayoría de las circunstancias.	Al menos 1 vez en el último año.
3	Posible	El evento podrá ocurrir en algún momento.	Al menos 1 vez en los últimos 2 años.
2	Improbable	El evento puede ocurrir en algún momento.	Al menos 1 vez en los últimos 5 años.
1	Rara vez	El evento puede ocurrir solo en circunstancias excepcionales (poco comunes o anormales).	No se ha presentado en los últimos 5 años.

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas, v6 - Dirección de Gestión y Desempeño Institucional, diciembre 2022

Niveles de calificación de impacto

La calificación del impacto para los riesgos de gestión y de seguridad de la información se tendrá en cuenta la siguiente escala, de acuerdo con la realidad de la institución.

Tabla 5. Calificación de impacto para riesgos de proceso y seguridad digital

Nivel	Impacto	Descripción Económica o Presupuestal	Descripción Reputacional
100%	Catastrófico	Pérdida económica superior a 1500 SMLV	Deterioro de imagen con efecto publicitario sostenido a nivel internacional.
80%	Mayor	Pérdida económica de 319 hasta 1500 SMLV	Deterioro de imagen con efecto publicitario sostenido a nivel Nacional o Territorial.
60%	Moderado	Pérdida económica de 21 hasta 318 SMLV	Deterioro de imagen con efecto publicitario sostenido a nivel Local o Sectores Administrativos.
40%	Menor	Pérdida económica de 11 hasta 20 SMLV	De conocimiento general de la entidad a nivel interno, Dirección General, Comités y Proveedores.
20%	Leve	Pérdida económica hasta 10 SMLV	Solo de conocimiento de algunos funcionarios.

Fuente: Oficina Asesora de Planeación

La calificación del impacto para los riesgos de corrupción se realiza aplicando la siguiente tabla de valoración establecida por Secretaria de Transparencia de la Presidencia de la Republica. Cada riesgo identificado es valorado de acuerdo con las preguntas, la tabla y la calificación obtenida se compara con la tabla de medición de impacto de riesgo de corrupción para obtener el nivel de impacto del riesgo.

Tabla 6. Calificación del Impacto para los riesgos de Corrupción

No.	Pregunta: Si el riesgo de corrupción se materializa podría		Respuesta	
			Si	No
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?			
Nivel	Descriptor	Descripción	Respuestas afirmativas	
1	Moderado	Genera medianas consecuencias sobre la entidad.	1 a 5	
2	Mayor	Genera altas consecuencias sobre la entidad.	6 a 11	
3	Catastrófico	Genera consecuencias desastrosas para la entidad.	12 a 19	

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas v6.

Criterios para la evaluación de impacto de pérdida de continuidad

La determinación de las prioridades de recuperación de servicios en caso de materialización de escenarios de pérdida de continuidad de negocio se realiza mediante la valoración del impacto percibido por los líderes de los procesos. Mediante mesa de trabajo los participantes califican los impactos en cada variable y definen el orden de recuperación de los servicios asignando la secuencia de reactivación de los mismos primero a los servicios con mayor impacto y de manera secuencia a los servicios con menor impacto percibido.

Tabla 7. Criterios para la evaluación de impacto de pérdida de continuidad

Criterio	Descripción
Financiero	Nivel de pérdidas económicas
Reputacional	Nivel de pérdida de la confianza de los grupos de valor en la entidad
Legal / Regulatorio	Nivel de incumplimiento de normas y regulaciones a las que está sometida la entidad
Contractual	Impactos asociados al incumplimiento de cláusulas en obligaciones contractuales
Misional	Nivel de incumplimiento o impacto percibido por imposibilidad de cumplir los objetivos y obligaciones misionales.

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas v6

Acciones ante los riesgos materializados

Ante la materialización de un riesgo se deberá medir el impacto y las consecuencias que puede ocasionar afectaciones a los objetivos de la Entidad, se revisarán y ajustarán los controles asociados determinando el grado de efectividad, eficiencia o eficacia, que garantice la mitigación de la ocurrencia. Para adelantar el análisis del riesgo y sus controles se deben considerar los siguientes aspectos:

- **Calificación del riesgo:** se logra a través de la estimación de la probabilidad de su ocurrencia y el impacto que puede causar la materialización del riesgo.
- **Bajo el criterio de probabilidad:** el riesgo se debe medir a partir de la cantidad de veces que se ejecuta cada una de sus acciones.

Se deberán tomar las medidas encaminadas a prevenir la ocurrencia como primera alternativa a considerar, se logra cuando al interior de los procesos se generan cambios sustanciales por mejoramiento, rediseño o eliminación, resultado de ajustes en los controles y acciones emprendidas.

Acciones a seguir en caso de materialización de riesgos de corrupción

En el evento de materializarse un riesgo de corrupción, es necesario realizar los ajustes necesarios con acciones, tales como:

- Informar a las autoridades de la ocurrencia del hecho de corrupción.
- Revisar el mapa de riesgos de corrupción, en particular, las causas, riesgos y controles.
- Verificar si se tomaron las acciones y se actualizó el mapa de riesgos de corrupción.
- Llevar a cabo un monitoreo permanente.

La Oficina de Control Interno debe asegurar que los controles sean efectivos, le apunten al riesgo y estén funcionando en forma oportuna y efectiva.

Las acciones adelantadas se refieren a:

- Determinar la efectividad de los controles.
- Mejorar la valoración de los riesgos.
- Mejorar los controles.
- Analizar el diseño e idoneidad de los controles y si son adecuados para prevenir o mitigar los riesgos de corrupción.
- Determinar si se adelantaron acciones de monitoreo.
- Revisar las acciones del monitoreo.

Cuando se materializan riesgos identificados en la matriz de riesgos institucionales se deben aplicar las acciones descritas en la tabla “acciones de respuesta a riesgos”.

Tabla 8. Acciones de respuesta a riesgos

Tipo de Riesgo	Responsable	Acción
Riesgo de Corrupción	Líder de Proceso	• Informar a la Oficina Asesora de Planeación como segunda línea de defensa en el tema de riesgos sobre el posible hecho encontrado y marcar en el SGI la alerta de posible materialización. • Una vez surtido el conducto regular establecido por la entidad y dependiendo del alcance (normatividad asociada al hecho de corrupción materializado), determinar la aplicabilidad del proceso disciplinario. • Identificar las acciones correctivas necesarias y documentarlas en el <i>plan de mejoramiento</i>.

Tipo de Riesgo	Responsable	Acción
		• Efectuar el análisis de causas y determinar acciones preventivas y de mejora. • Revisar los controles existentes y actualizar el mapa de riesgos.
	Oficina de Control Interno	• Informar al líder del proceso y a la segunda línea de defensa, quienes analizarán la situación y definirán 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), determinar la aplicabilidad del proceso disciplinario. • Informar a discreción los posibles actos de corrupción al ente de control.
Riesgos de Gestión y Seguridad digital	Líder de Proceso	• Informar a la Oficina Asesora de Planeación como segunda línea de defensa, el evento o materialización de un riesgo. • Proceder de manera inmediata a aplicar el <i>plan de contingencia o de tratamiento de incidentes de seguridad de la información</i> que permita la continuidad del servicio o el restablecimiento de este (si es el caso) y documentar en el plan de mejoramiento. • Realizar los correctivos necesarios frente al cliente e iniciar el análisis de causas y determinar acciones correctivas, preventivas, y de mejora, así como la revisión de los controles existente, documentar en el plan de mejoramiento institucional y actualizar el mapa de riesgos. • Dar cumplimiento al procedimiento plan de mejoramiento.

Tipo de Riesgo	Responsable	Acción
Riesgos de Gestión y Seguridad digital	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. • Verificar que se tomen las acciones y se actualice el mapa de riesgos correspondiente. • Si la materialización de los riesgos es el resultado de una auditoría realizada por la Oficina de Control Interno, esta verificará el cumplimiento del plan de mejoramiento y realizará el seguimiento de acuerdo con el procedimiento.
Riesgos de continuidad de negocio	Comité de crisis	• Activar el plan de continuidad de negocio

Fuente: Oficina Asesora de Planeación

Tabla 9. Seguimiento al mapa de riesgos y controles

Tipo de Riesgo	Zona de Riesgo Residual	Estrategia de Tratamiento - Controles
Riesgos de Gestión, y Seguridad digital	Baja	Se realiza seguimiento a los controles con periodicidad SEMESTRAL y se registran sus avances en el módulo de riesgos- SGI.
	Moderada	Se realiza seguimiento a los controles con periodicidad TRIMESTRAL y se registran sus avances en el módulo de riesgos- SGI.
	Alta	Se realiza seguimiento a los controles con periodicidad BIMESTRAL y se registran sus avances en el módulo de riesgos- SGI
	Extrema	Se realiza seguimiento a los controles con periodicidad MENSUAL y se registra en el módulo de riesgos – SGI.
Riesgos de Corrupción	Todos los riesgos de corrupción, independiente de la zona de riesgo en la que se encuentran debe tener un seguimiento MENSUAL y se registra en el módulo de riesgos – SGI.	

Fuente: Oficina Asesora de Planeación

Estrategia de seguimiento al plan de acción

Tabla 10. Estrategia de seguimiento al plan de acción

Tipo de Riesgo	Zona de Riesgo Residual o severidad	Estrategia de Tratamiento – Plan de Acción
Riesgos de Gestión, y Seguridad digital	Baja	No se debe realizar plan de acción porque está dentro del nivel de aceptación del riesgo por Función Pública.
	Moderada	El líder del proceso define acciones que permita mitigar el riesgo residual. Asimismo, determina la fecha de inicio y finalización de estas y establece los seguimientos que va a realizar durante la ejecución de la acción correspondiente a su avance, el cual se debe reportar junto con el seguimiento al mapa de riesgo y controles. Después de haber implementado la acción debe realizar un seguimiento con el fin de evaluar la efectividad del plan de acción.
	Alta Extrema	

Fuente: Oficina Asesora de Planeación

Anexos

Para una mayor comprensión de la política de operación para la administración del riesgo, se define que los anexos son parte fundamental de este documento técnico, por tanto, se recomienda su consulta y conocimiento por parte de todos los servidores públicos de la Entidad.

- Manual operativo MIPG

https://www.funcionpublica.gov.co/documents/34645357/34702994/Modelo_integrado_pla_neacion_gestion.pdf/7f3d55ea-4ad6-3bdc-3f05-a23d287ca69b?t=1615223466439

- Manual Metodología de riesgos

https://www.funcionpublica.gov.co/documents/34645357/34702994/Manual_metodologia_r iesgos.pdf.pptx/8b3d4a02-7c0d-41a7-b609-3752cb063bc8?t=1536162961916

- Guía para la Administración del riesgo de FP

https://www.funcionpublica.gov.co/documents/34645357/34702994/Guia_externa_adminis tracion_riesgo_direccinamiento_estrategico.pdf/0330fa64-0a6a-4772-887f-27aae325afa5?t=1614199851989

- Matriz de autoridad y responsabilidad

<https://www.funcionpublica.gov.co/web/intranet/manuales-proceso-direccionamiento-estrategico>

- Manual del usuario – módulo de riesgos SGI

https://www.funcionpublica.gov.co/documents/34645357/34702994/Manual_usuario_sgi modulo_riegos_direccionamiento.pdf/e9a51e27-30af-4045-b0b2-53713707d456?t=1536164158725



**Paisaje Cultural Cafetero
Patrimonio de la Humanidad
Declarado por la UNESCO**

- Plan de Continuidad

<https://www.funcionpublica.gov.co/plan-de-continuidad>

- Procedimiento Administración del plan de mejoramiento institucional

<https://www.funcionpublica.gov.co/web/intranet/procedimiento-administracion-plan-mejoramiento-institucional>

Política de Administración de Riesgos en Función Pública

Versión 18
Proceso de Direccionamiento Estratégico
JUNIO de 2023