Política de Operación para la Administración del Riesgo en Función Pública

Documento Técnico
Oficina Asesora de Planeación

Julio de 2020

Tabla de contenido

“Función Pública se compromete a administrar adecuadamente los riesgos de gestión, de corrupción y de Seguridad Digital, asociados a los objetivos estratégicos, planes, proyectos y procesos institucionales, acatando la metodología propia para su gestión, determinando las acciones de control detectivas y preventivas oportunas para evitar la materialización y la actuación correctiva inmediata ante las eventualidades para mitigar las posibles consecuencias a fin de mantener los niveles de riesgo aceptables”

Introducción

El presente documento establece los lineamientos para la identificación, análisis, valoración, evaluación , tratamiento y respuesta a los riesgos y escenarios de pérdida de continuidad de negocio que puedan afectar la misión, el cumplimiento de los objetivos estratégicos y la gestión de los procesos, proyectos y planes institucionales, tomando como referencia las directrices del Modelo Integrado de Planeación y Gestión- MIPG, la responsabilidad de las líneas de defensa definidas en el Modelo Estándar de Control Interno – MECI, los requerimientos de la Guía para la administración del riesgo de FP y el Modelo de seguridad y privacidad de la información de la estrategia de Gobierno Digital,

Objetivo

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 consecuencia 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

Alcance

La política de operación de riesgos es aplicable a todos los servicios, procesos, proyectos y planes de la entidad durante el desarrollo de la gestión planificada y a todos los servidores públicos en el ejercicio de sus funciones.

Glosario

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

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

Contingencia: Posible evento futuro, condición o eventualidad

Continuidad: Capacidad de una organización para continuar la entrega de productos o servicios a niveles aceptables después de una crisis

Crisis (Emergencia): Ocurrencia o evento repentino, urgente, generalmente inesperado que requiere acción inmediata

CGDI: Comité de Gestión y Desempeño Institucional

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

MECI: Modelo Estándar de Control Interno

OTIC: Oficina de las Tecnologías de la Información y las Comunicaciones

OAC: Oficina Asesora de Comunicaciones

OAP: Oficina Asesora de Planeación

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.

SGI: Sistema Gestión Institucional

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.

Responsabilidades

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

Líneas de Defensa	Responsable	Responsabilidad frente al riesgo
Línea Estratégica	Comité Directivo Comité de Gestión y Desempeño Institucional Comité Institucional de Control Interno	• Definir y aprobar el marco general para la gestión del riesgo, la gestión de la continuidad del negocio y el control • 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. • Definir y aprobar la política para la administración del riesgo • Garantizar el cumplimiento de los planes de la entidad
Primera Línea	Líderes de Proceso Responsable del proyecto	• Identificar, valorar, evaluar y actualizar cuando se requiera, los riesgos que pueden afectar los objetivos, programas, proyectos y planes asociados a su proceso. • Definir, adoptar, aplicar y hacer seguimiento a los controles para mitigar los riesgos identificados y proponer mejoras para su gestión. • 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 de acuerdo con su competencia y alcance la documentación de continuidad de negocio • Desarrollar ejercicios de autoevaluación para establecer la eficiencia, eficacia y efectividad de los controles seleccionados para el tratamiento de los riesgos identificados y los planes de preparación frente a la pérdida de continuidad de negocio. • Informar a la oficina de planeación (segunda línea) sobre los riesgos materializados en los objetivos, programas, proyectos y planes de los procesos a cargo. • Reportar en el SGI los avances y evidencias de la gestión de los riesgos dentro de los plazos establecidos.
		• Asesorar a la línea estratégica en el análisis del contexto interno y externo, para la definición de la política de riesgo, el establecimiento de los niveles de impacto y el nivel de aceptación del riesgo residual. • Consolidar el mapa de riesgos institucional, riesgos de mayor criticidad frente al logro de los objetivos) y presentarlo para análisis y seguimiento ante el CGDI • Actualizar la documentación que soporta la estrategia de continuidad de negocio • Presentar al CICCI el resultado de la medición del nivel de eficacia de los controles para el tratamiento de los riesgos identificados en las áreas en los diferentes niveles de operación de la entidad.

Segunda Línea	Oficina Asesora de Planeación	• 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 CICI. • Actualizar, según se requiera, los escenarios de riesgo y la documentación asociada al plan de continuidad de negocio bajo su responsabilidad.
Segunda Línea	Secretaria General, Coordinadores de Gestión Contractual, Administrativa, Financiera, Servicio al Ciudadano, Gestión Documental, Talento Humano y Defensa Jurídica; Jefes de la OTIC, OAC y OAP; Responsable del proyecto	• Acompañar a los líderes de procesos en la identificación, análisis, valoración, evaluación del riesgo, la definición de controles y las estrategias de continuidad de negocio asociadas a los escenarios de continuidad de negocio bajo su responsabilidad y los temas a su cargo. • Monitorear los riesgos identificados y controles definidos por la primera línea de defensa acorde con la estructura de los temas a su cargo. • Realizar el seguimiento al mapa de riesgos de su proceso. • Reportar en el módulo de riesgos del aplicativo SGI o delegar a un profesional de la dependencia o grupo a su cargo, el registro de los avances en la gestión del riesgo. • Proponer las acciones de mejora a que haya lugar posterior al análisis, valoración, evaluación o tratamiento del riesgo. • Actualizar, según se requiera, los escenarios de riesgo y la documentación asociada al plan de continuidad de negocio bajo su responsabilidad • 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 de gestión del riesgo asociado a su responsabilidad. • Participar en las pruebas del plan de continuidad de negocio y en la implementación • El Coordinador del Grupo de Defensa Jurídica tendrá el compromiso de identificar, analizar, valorar y evaluar los riesgos y

	Delegados de riesgos en cada proceso	controles asociados a su gestión con enfoque en la prevención del daño antijurídico • Comunicar al equipo de trabajo a su cargo la responsabilidad y resultados de la gestión del riesgo.
Tercera Línea	Oficina de Control Interno	• Proporcionar aseguramiento objetivo sobre la eficacia de la gestión del riesgo y control, con énfasis en el diseño e idoneidad de los controles establecidos en los procesos. • Proporcionar aseguramiento objetivo en las áreas identificadas no cubiertas por la segunda línea de defensa • Asesorar 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 CICI. • Recomendar mejoras a la política de operación para la administración del riesgo

De igual manera, la *Oficina Asesora de Planeación* lleva a cabo las siguientes acciones durante el acompañamiento para la identificación y administración del riesgo:

- Socializar anualmente la metodología de riesgos, los lineamientos de la primera línea de defensa frente al riesgo, objetivo del proceso, comunicación de los planes y proyectos del proceso asesorado.
- Capacitar al grupo de trabajo de cada dependencia en la herramienta SGI para la gestión del riesgo
- Liderar las mesas de trabajo de identificación del riesgo
- Liderar las mesas de trabajo para determinación del análisis de impacto del negocio, documentación de los escenarios de riesgo y plan de continuidad de negocio institucional.
- Verificar que las acciones de control se documenten conforme a los requerimientos de la metodología
- Identificar claramente, junto con el equipo de trabajo, los responsables de las acciones y las fechas de realización, y registrarlas en el SGI
- Elaborar el mapa de riesgos de proceso con toda la información respectiva, a partir de la información construida con los equipos de trabajo
- Documentar los escenarios de perdida de continuidad de negocio que se utilizan para el desarrollo y prueba del plan de continuidad de negocio
- Presentar la propuesta para aprobación del líder del proceso
- Una vez aprobado, comunicar al líder del proceso los resultados de las mesas de identificación y recordar la importancia de socializarlos al interior de su dependencia
- Revisar que el cargue de información en el SGI esté acorde con lo aprobado
- Identificar, socializar y publicar el mapa de riesgos institucional a partir de los mapas de proceso, con los riesgos altos, extremos y de corrupción.

Por su parte, los *líderes de proceso* tienen la responsabilidad de

- Asegurar que al interior de su grupo de trabajo se reconozca el concepto de “administración del riesgo”, la política y la metodología definida, los actores y el entorno del proceso aprobados por la primera línea de defensa

- Delegar, por parte del líder del proceso, el (los) profesionales que se encargarán de la identificación, monitoreo, reporte y socialización del riesgo asociados.

Adicionalmente, la matriz de responsabilidad y autoridad de Función Pública define los cargos que pueden identificar, valorar, evaluar y definir controles y reportar los riesgos institucionales en el módulo de riesgos del SGI, por lo cual dicha matriz hace parte de este documento.

http://www.funcionpublica.gov.co/documents/34645357/34702994/Niveles_autoridad_responsabilidad_modulo_sgi.pdf/eb96d8e5-1565-4745-93ac-cffa63db02d9?t=1556125180553

Escenarios de pérdida de continuidad

Los escenarios de riesgo corresponden a descripciones de situaciones que agrupa la ocurrencia de uno o más riesgos que generan la pérdida de continuidad en las actividades institucionales. La entidad adopta el siguiente conjunto de escenarios de riesgo estandarizados para el diseño de la estrategia de continuidad de negocio.

Escenario	Descripción
Emergencia Social	Imposibilidad de uso de las instalaciones debido a revueltas sociales, asonadas o pérdida del orden público que hace imposible la prestación del servicio o generación del producto.
Colapso de infraestructura física	Imposibilidad de acceso o abandono súbito de las instalaciones debido a caso fortuito, fenómeno natural o fuerza mayor
Desastre Tecnológico	Pérdida total de la capacidad tecnológica o de los procesos institucionales para prestar los servicios o generar los productos
Crisis Financiera	Inexistencia de los bienes y servicios necesarios para el normal funcionamiento de la entidad que impacta la disponibilidad de recursos financieros, humanos, físicos y tecnológicos
Pandemia	Crisis sanitaria que impide el funcionamiento de los procesos institucionales, incluye pandemias y epidemias declaradas por los organismos de salud del Estado.

Cuando se presentan eventos que materializan uno o más de los escenarios de continuidad del negocio la Entidad evalúa las características de la emergencia para autorizar la activación del plan de continuidad, designar recursos y autorizar cualquier comunicación oficial hacia todos los grupos de valor, una vez declarada oficialmente la emergencia, se aplican las acciones de respuesta definidas en el plan de continuidad de negocio para dar respuesta a la misma.

Etapas para la gestión del riesgo

La gestión de riesgos comprende las actividades de análisis del contexto interno y externo, identificación y análisis del riesgo, valoración, evaluación, definición de controles para el tratamiento y seguimiento. Las diferentes etapas con sus entradas, instrumentos y resultados se describen en el Manual Metodología de Riesgos.

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

Tablas Calificación Impacto

Las tablas de calificación del Impacto definidas para los Riesgos de Gestión, Corrupción y Seguridad Digital se definen así:

Riesgos de Gestión

PROBABILIDAD		IMPACTO		
Categoría	**Descripción**	**Categoría**	**Descripción Cuantitativa**	**Descripción Cualitativa**
NIVEL 5. CASI SEGURO	Se espera que el evento ocurra en la mayoría de las circunstancias - Más de 1 vez al año.	**NIVEL 5. CATASTRÓFICO**	*Impacto que afecte la ejecución presupuestal en un valor igual o superior al 50% * Pérdida de cobertura en la prestación de los servicios de la entidad en un valor igual o superior al 50% * Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor igual o superior al 50% * Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor igual o superior al 50% del presupuesto general de la entidad.	*Interrupción de las operaciones de la Entidad por más de cinco (5) días. - Intervención por parte de un ente de control u otro ente regulador. - Pérdida de Información crítica para la entidad que no se puede recuperar. - Incumplimiento en las metas y objetivos institucionales afectando de forma grave la ejecución presupuestal. - Imagen institucional afectada en el orden nacional o regional por actos o hechos de corrupción comprobados.
NIVEL 4. PROBABLE	Es viable que el evento ocurra en la mayoría de las circunstancias - Al menos 1 vez en el último año.	**NIVEL 4. MAYOR**	* Impacto que afecte la ejecución presupuestal en un valor igual o mayor al 20% e inferior al 50% * Pérdida de cobertura en la prestación de los servicios de la entidad en un valor igual o mayor al 20% e inferior al 50% * Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor igual o mayor al 20% e inferior al 50% * Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor igual o mayor al 20% e inferior al 50% del presupuesto general de la entidad.	* Interrupción de las operaciones de la Entidad por más de dos (2) días. - Pérdida de información crítica que puede ser recuperada de forma parcial o incompleta. - Sanción por parte del ente de control u otro ente regulador. - Incumplimiento en las metas y objetivos institucionales afectando el cumplimiento en las metas de gobierno. - Imagen institucional afectada en el orden nacional o regional por incumplimientos en la prestación del servicio a los usuarios o ciudadanos.
NIVEL 3. POSIBLE	El evento podrá ocurrir en algún momento - Al menos 1 vez en los últimos 2 años.	**NIVEL 3. MODERADO**	* Impacto que afecte la ejecución presupuestal en un valor igual o mayor al 10% y menor al 20% * Pérdida de cobertura en la prestación de los servicios de la entidad en un valor igual o mayor al 10% y menor al 20% * Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor igual o mayor al 10% y menor al 20% * Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor igual o mayor al 10% y menor al 20%del presupuesto general de la entidad.	* Interrupción de las operaciones de la Entidad por un (1) día. - Reclamaciones o quejas de los usuarios que podrían implicar una denuncia ante los entes reguladores o una demanda de largo alcance para la entidad. - Inoportunidad en la información ocasionando retrasos en la atención a los usuarios. - Reproceso de actividades y aumento de carga operativa. - Imagen institucional afectada en el orden nacional o regional por retrasos en la prestación del servicio a los usuarios o ciudadanos. - Investigaciones penales, fiscales o disciplinarias.
NIVEL 2. IMPROBABLE	El evento puede ocurrir en algún momento - Al menos 1 vez en los últimos 5 años.	**NIVEL 2. MENOR**	* Impacto que afecte la ejecución presupuestal en un valor igual o mayor al 1% y menor al 10% - Pérdida de cobertura en la prestación de los servicios de la entidad en un valor igual o mayor al 1% y menor al 10% - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor igual o mayor al 1% y menor al 10% - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≤1%del presupuesto general de la entidad.	* Interrupción de las operaciones de la Entidad por algunas horas. - Reclamaciones o quejas de los usuarios que implican investigaciones internas disciplinarias. - Imagen institucional afectada localmente por retrasos en la prestación del servicio a los usuarios o ciudadanos.
NIVEL 1. RARA VEZ	El evento puede ocurrir solo en circunstancias excepcionales (poco comunes o anormales). - No se ha presentado en los últimos 5 años	**NIVEL 1. INSIGNIFICANTE**	* Impacto que afecte la ejecución presupuestal en un valor menor al 1% * Pérdida de cobertura en la prestación de los servicios de la entidad ≤1%. * Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor menor al 1% * Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor menor al 1% del presupuesto general de la entidad.	*No hay interrupción de las operaciones de la entidad. - No se generan sanciones económicas o administrativas. - No se afecta la imagen institucional de forma significativa.

Medición de impacto de riesgos de Corrupción

La medición del impacto de los riesgos de corrupción se realiza aplicando la siguiente tabla de valoración. 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.

Medición de Impacto Riesgo de Corrupción			
Descriptor	**Descripción**	**Nivel**	**Respuestas Afirmativas**
Moderado	Afectación parcial al proceso y a la dependencia Genera medianas consecuencias para la entidad.	5	1 – 5
Mayor	Impacto negativo de la Entidad Genera altas consecuencias para la entidad.	10	6 - 11
Catastrófico	Consecuencias desastrosas sobre el sector Genera consecuencias desastrosas para la entidad.	20	12 - 19

N	Pregunta Si el riesgo se materializa podria?	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 misión del sector al cual pertenece la Entidad ?		
5	¿Generar perdida de confianza de la Entidad, afectando su reputación?		
6	¿Generar perdida 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 perdida del bien o servicios o los recursos públicos?		
9	¿Generar perdida 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 perdida de credibilidad del sector?		
16	¿Ocasionar lesiones físicas o perdida de vidas humanas ?		
17	¿Afectar la imagen regional?		
18	¿Afectar la imagen nacional?		
19	¿Generar daño ambiental?		

Valoración de impacto de Riesgos Seguridad Digital

Criterios de Impacto para Riesgos de Seguridad Digital			
Categoría	**Descripción Cuantitativa**	**Descripción Cualitativa**	**Nivel**
CATASTRÓFICO	Afectación en un valor igual o superior al 50%de la población. Afectación en un valor igual o superior al 50% del presupuesto de seguridad de la información en la entidad. Afectación muy grave del medio ambiente que requiere > 3 años de recuperación.	Afectación muy grave de la integridad de la información debido al interés particular de los empleados y terceros. Afectación muy grave de la disponibilidad de la información debido al interés particular de los empleados y terceros. Afectación muy grave de la confidencialidad de la información debido al interés particular de los empleados y terceros. Interrupción de las operaciones de la Entidad por más de cinco 5 días	5
MAYOR	Afectación en un valor igual o mayor al 20% e inferior al 50% de la población. Afectación en un valor igual o mayor al 20% e inferior al 50% del presupuesto de seguridad de la información en la entidad. Afectación importante del medio ambiente que requiere de 1 a 3 años de recuperación.	Afectación grave de la integridad de la información debido al interés particular de los empleados y terceros. Afectación grave de la disponibilidad de la información debido al interés particular de los empleados y terceros. Afectación grave de la confidencialidad de la información debido al interés particular de los empleados y terceros. Interrupción de las operaciones de la Entidad entre 2 y 4 días	4
MODERADO	Afectación en un valor igual o mayor al 10% y menor al 20% de la población. Afectación en un valor igual o mayor al 10% y menor al 20% del presupuesto de seguridad de la información en la entidad. Afectación leve del medio ambiente requiere de 3,1 a 1 año de recuperación.	Afectación moderada de la integridad de la información debido al interés particular de los empleados y terceros. Afectación moderada de la disponibilidad de la información debido al interés particular de los empleados y terceros. Afectación moderada de la confidencialidad de la información debido al interés particular de los empleados y terceros. Interrupción de las operaciones de la Entidad por un (1) día.	3
MENOR	Afectación en un valor igual o mayor al 1% y menor al 10%de la población. Afectación en un valor igual o mayor al 1% y menor al 10%del presupuesto de seguridad de la información en la entidad. Afectación leve del medio ambiente requiere de 1 a 3 meses de recuperación.	Afectación leve de la integridad. Afectación leve de la disponibilidad. Afectación leve de la confidencialidad. Interrupción de las operaciones de la Entidad hasta por 8 horas (1 jornada laboral)	2
INSIGNIFICANTE	Afectación en un valor menor al 1% de la población. Afectación en un valor menor al 1% del presupuesto de seguridad de la información en la entidad. No hay afectación medioambiental.	Sin afectación de la integridad. Sin afectación de la disponibilidad. Sin afectación de la confidencialidad No hay interrupción de las operaciones de la entidad	1

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.

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.

De igual manera, en el Manual Metodología de Riesgos de FP (Numerales 5.2, 5.3 y 5.4 respectivamente) se amplía esta información:

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

Acciones ante los riesgos materializados

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 1 Acciones de respuesta a riesgos

Tipo de Riesgo	Responsable	Acción
Riesgo 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
Riesgos de Gestión y Seguridad digital (Zona Extrema, Alta y Moderada)	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.
Riesgos de Gestión y Seguridad digital (Zona Extrema, Alta y Moderada)		• Informar al Proceso de Direccionamiento Estratégico sobre el hallazgo y las acciones tomadas.

Riesgos de Gestión y Seguridad digital (Zona Baja)		• 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.
Riesgos de Gestión y Seguridad digital (Zona Extrema, Alta y Moderada)	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 Proceso y Seguridad digital (Zona Baja)		• 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.

Estrategias para la aceptación del riesgo residual

Acorde con los riesgos residuales aprobados por el Comité Institucional de Coordinación de Control Interno, se debe definir la periodicidad de seguimiento y estrategia de tratamiento a los riesgos residuales aceptados, así:

Tabla 2 Matriz de calificación de nivel de criticidad de riesgo

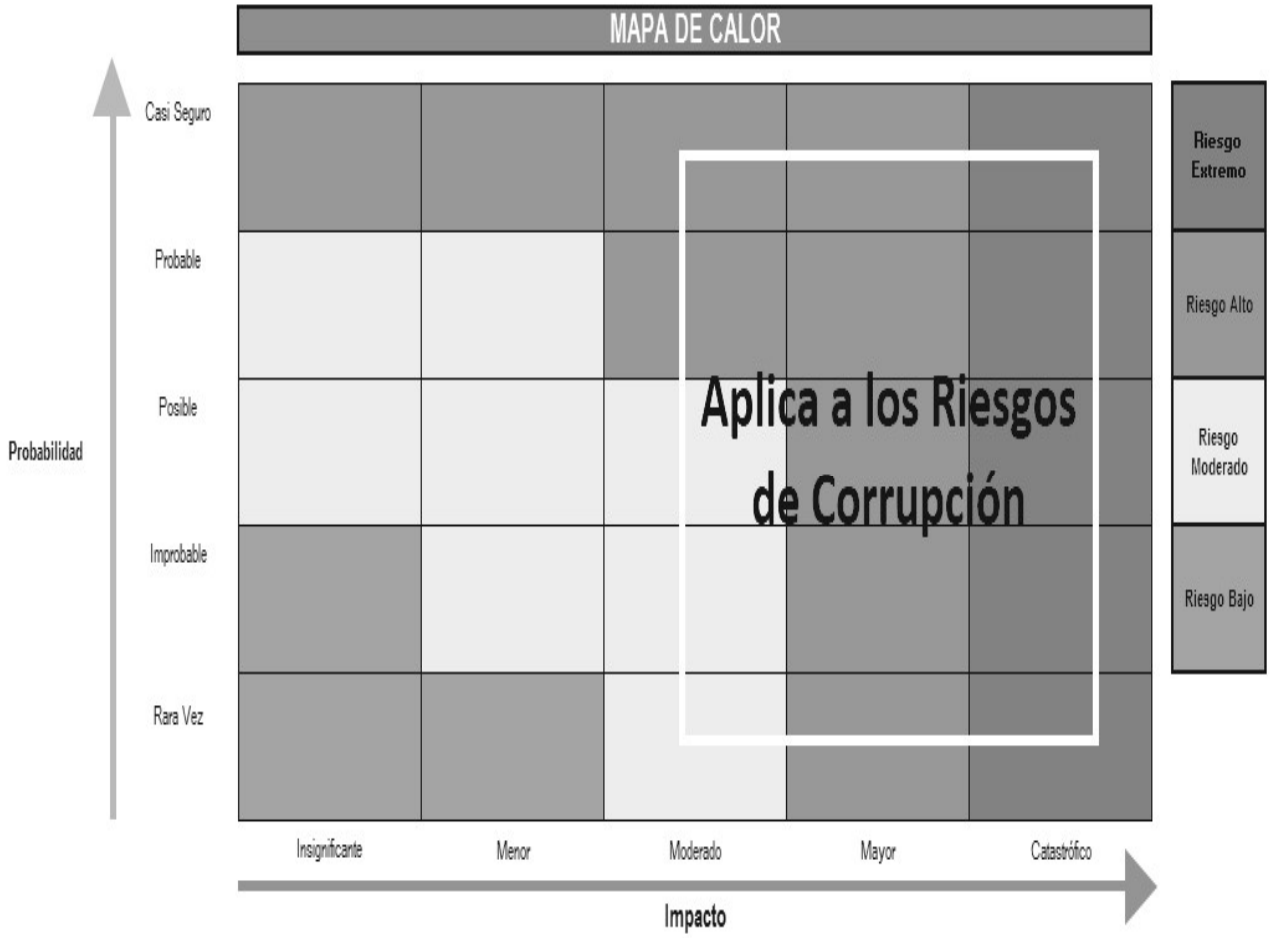

Tabla 3 Estrategias de tratamiento de riesgo

Tipo de Riesgo	Zona de Riesgo Residual	Estrategia de tratamiento
Riesgos de Gestión y Seguridad digital	Baja	Se **ACEPTA** el riesgo y se administra por medio de las actividades propias del proyecto o proceso asociado y se realiza en el reporte mensual de su desempeño.
	Moderada	Se establecen acciones de control preventivas que permitan **REDUCIR** la probabilidad o el impacto de ocurrencia del riesgo, se hace seguimiento **BIMESTRAL** y se registran sus avances en el Módulo de Riesgos- SGI
	Alta y Extrema	Se debe incluir el riesgo tanto en el Mapa de riesgo del Proceso como en el Mapa de Riesgo Institucional y se establecen acciones de Control Preventivas que permitan **EVITAR** la materialización del riesgo. Se monitorea **MENSUALMENTE** y se registra en el Módulo de Riesgos - SGI
Riesgos de Corrupción	Baja	Ningún riesgo de corrupción podrá ser aceptado. Periodicidad de seguimiento **MENSUAL** para evitar a toda costa su materialización por parte de los procesos a cargo de estos.
	Moderada	Se establecen acciones de control preventivas que permitan **REDUCIR** la probabilidad de ocurrencia del riesgo. Periodicidad de seguimiento **MENSUAL** para evitar a toda costa su materialización por parte de los procesos a cargo de estos y se registra en el Módulo de Riesgos - SGI
	Alta y Extrema	Se adoptan medidas para: **REDUCIR** la probabilidad, el impacto o ambos factores del riesgo; la estrategia conlleva a la implementación de controles. **EVITAR** Se abandonan o modifican las actividades que dan lugar al riesgo, decidiendo no iniciar, no continuar o modificar de forma segura la actividad que causa el riesgo. **COMPARTIR** con un tercero el tratamiento de una parte del riesgo para reducir la probabilidad, el impacto o ambos factores. Periodicidad de seguimiento **MENSUAL** para evitar a toda costa su materialización por parte de los procesos a cargo de los mismos y se registra en el Módulo de Riesgos - SGI

Seguimiento a las acciones de control del riesgo en cada proceso

- Según la periodicidad definida para cada riesgo, el delegado de riesgos en cada proceso y el líder del mismo verifica las acciones preventivas y registra el avance junto con la evidencia en el SGI.
- El delegado de riesgo en cada proceso y el líder del mismo analizan los resultados del seguimiento y establece acciones inmediatas ante cualquier desviación
- El líder del proceso comunica las desviaciones según el nivel de aceptación del riesgo al interior de su dependencia y las acciones a seguir.
- El líder del proceso se asegura que se documenten las acciones de corrección o prevención en el plan de mejoramiento
- El delegado de riesgo en cada proceso y el líder del mismo revisa y actualiza, con el acompañamiento de la OAP, el mapa de riesgo cuando se modifique las acciones o la ubicación del riesgo

Periodo de revisión riesgos institucionales

Los riesgos se identifican y/o validan en cada vigencia, atendiendo la metodología vigente, una vez se defina el plan de acción institucional, asegurando la articulación de éstos con los compromisos de cada proceso.

Herramienta para la gestión del riesgo

Función Pública determina que el Módulo de Riesgos del SGI es la herramienta para identificar, valorar, evaluar y administrar los riesgos, de corrupción y de seguridad digital, por tanto, toda información asociada con los riesgos es provista por dicha herramienta, para lo cual la Oficina Asesora de Planeación identifica los requerimientos funcionales, revisa periódicamente su adecuado funcionamiento y cargue de información y dispone un manual de uso para el servicio de todos los procesos.

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

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
- Metodología de riesgos
- Guía para la Administración del riesgo de FP

- Matriz de autoridad y responsabilidad
- Manual del usuario – módulo de riesgos SGI
- Manual Metodología de gestión de riesgo

Oficina Asesora de Planeación
Abril de 2020