CONTROL DE CAMBIOS

No. DE ACTA DE APROBACIÓN	FECHA	VERSIÓN	DESCRIPCIÓN
047	14/12/2018	1.0	Adopción política
003	25/01/2021	2.0	Se separan en dos documentos la política y la Guía de metodológica para la administración de riesgos, se ajustan el documento según la guía para la Administración del riesgo y diseño de controles en entidades públicas Paso 1: Política Administración de Riesgos Cambia de código pasa de PE01-PR03-P01 a PE01-PL01
028	23/08/2021	3.0	Se actualiza política de gestión de riesgos dando cumplimiento a la Guía para la administración del riesgo y el diseño de controles en las entidades públicas Versión 5 de 2020
09	6/04/2022	4.0	Se actualiza la política de gestión de riesgos incluyendo riesgo asociado al lavado de activos (LA) y financiación del terrorismo (FT) Se actualiza incluyendo actividades de comunicación en la gestión del riesgo. Se realizan cambios de forma relacionados a la organización del documento.

AUTORIZACIONES

ELABORÓ:	REVISÓ	APROBÓ
ÁREA TÉCNICA	**OFICINA ASESORA DE PLANEACIÓN**	**LÍDER DEL PROCESO**
Nombre: Ximena A Castro P	**Nombre:** Sara Sofía Lancheros Ramírez Claudia Patricia Guerrero Chaparro	**Nombre:** Ingrid Elizabeth Torres Rodríguez
Firma:	**Firma:** Sara Lancheros Ramirez	**Firma:**
Cargo: Colaborador Profesional Oficina Asesora de Planeación	**Cargo:** Profesional Oficina Asesora de Planeación/ Asesora Oficina de Control Interno	**Cargo:** Jefe Oficina Asesora de Planeación

INTRODUCCIÓN

El Instituto de Protección y Bienestar Animal define su política y los lineamientos para la administración del riesgo, tomando como referente lo establecido en el Modelo Integrado de Planeación y Gestión aplicados en todos los procesos institucionales, ajustándolos a las líneas de defensa que articulan la identificación, tratamiento, valoración y seguimiento de los riesgos de gestión, corrupción y seguridad digital.

En este sentido todos los procesos del Instituto establecen los mecanismos para la identificación, valoración y tratamiento de los riesgos que puedan afectar la misión y el cumplimiento de los objetivos institucionales en cumplimiento de los proyectos y planes de trabajo.

Para la realización de las acciones de control se definen actuaciones detectives y preventivas, así como la actuación correctiva y oportuna ante la materialización de los riesgos identificados.

En general, se tienen en cuenta para gestionar adecuadamente los riesgos del instituto, los objetivos estratégicos, los niveles de responsabilidad frente al manejo de los riesgos y los mecanismos de comunicación utilizados para dar a conocer la política a todos los niveles de la entidad.

El Gobierno Nacional, acogiendo la recomendación No 2 del GAFI, expidió el documento CONPES 3793 de 2013, mediante al cual define y adopta la "Política Nacional Antilavado de Activos y Contra La Financiación del Terrorismo" en armonía con lo establecido en el artículo 113 de la Constitución Política de Colombia

Por otra parte, la Política Pública Distrital de Transparencia, Integridad y No Tolerancia con la Corrupción surge como un medio para robustecer la gobernabilidad, lo cual implica el fortalecimiento de las instituciones distritales, la promoción de alianzas estratégicas y un papel activo de la ciudadanía. La política es resultado del reconocimiento de la presencia de prácticas corruptas y la decisión de la administración distrital de emprender una acción política e institucional articulada frente a la problemática, por ello la importancia de la cooperación entre entidades del estado, para debilitar estos delitos.

La Secretaría General de la Alcaldía Mayor de Bogotá D.C., a través del documento denominado Ruta Metodológica para la Implementación del SARLAFT en las Entidades Distritales recomendó como una buena práctica que las entidades distritales asocien y articulen a su gestión de riesgos, los criterios para la identificación, análisis y evaluación de riesgos asociados a LA/ FT, en el marco del fortalecimiento del sistema de control interno bajo el Modelo Estándar de Control Interno MECI, así como al esquema de líneas de defensa enmarcadas en el Modelo Integrado de Planeación y Gestión MIPG.

OBJETIVO

El Instituto de Protección y Bienestar Animal en cumplimiento de su planeación estratégica, el fortalecimiento del control interno, el mejoramiento continuo y el logro de sus objetivos estratégicos, tiene como propósito el establecimiento y actualización de la política para la administración de los riesgos de gestión, conflictos de interés, corrupción, seguridad de la información, riesgo asociado al lavado de activos (LA) y Financiación del Terrorismo (FT) a través de su tratamiento, manejo y seguimiento, en aras de gestionarlos a un nivel aceptable.

ALCANCE

La presente política es extensible y aplicada en todos los niveles, procesos y sedes del Instituto a través de los servidores públicos y contratistas, que presten sus servicios en la Entidad

POLÍTICA DE ADMINISTRACIÓN DE RIESGO

El Instituto Distrital de Protección y Bienestar Animal, se compromete a realizar gestión a los riesgos relacionados con las actividades a ejecutar desde sus procesos estratégicos, misionales, apoyo, evaluación y control, para garantizar la continuidad de las operaciones y el cumplimiento de los objetivos, metas y la transparencia en la gestión. En el proceso de implementar la adecuada gestión de los riesgos, los líderes de los procesos tendrán en cuenta la importancia del riesgo identificado analizando el efecto que puede tener, la probabilidad e impacto de este y las estrategias para combatirlo.

TIPOLOGÍA DE RIESGOS.

Calidad: relacionados con los atributos de calidad establecidos en MIPG, las políticas de aseguramiento y control de calidad

Contratación: relacionado con los atrasos o incumplimientos de las etapas contractuales en cada vigencia

Comunicación: relacionado con los canales, medios y oportunidades para informar durante las diferentes etapas de un proyecto

Corrupción: posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.

Cumplimiento y conformidad: se asocian con los requisitos legales, contractuales, de ética pública y en general con su compromiso ante la comunidad

Estratégicos: asociado a la administración de la Entidad, a la misión y el cumplimiento de los objetivos estratégicos, la definición de políticas, y el diseño de lineamientos que respondan a las necesidades de los grupos de valor e interés

Financieros: relacionado con el manejo de recursos, la ejecución presupuestal, la elaboración de los estados financieros, los pagos, manejos de excedentes de tesorería y el manejo de los bienes

Imagen: relacionado con la percepción y la confianza por parte de los grupos de valor frente a la Entidad

Información: se asocia a la disponibilidad, confiabilidad e integridad de la información agregada y desagregada

Integración: Se refiere a la integración de sistemas, áreas, entidades, etapas y elementos que se requieran coordinar para el desarrollo de un proyecto

Operativos: riesgos provenientes del funcionamiento y operatividad de los procesos, sistemas de información, estructura de la entidad y articulación entre dependencias

Recurso Humano: Se asocia a la cualificación, competencia y disponibilidad de personal requerido para realizar un proyecto o función

Tecnológicos: relacionados con la capacidad tecnológica para satisfacer sus necesidades actuales y futuras y el cumplimiento de la misión

Seguridad de la información: potencial de que las amenazas exploten la vulnerabilidad de un activo de información o grupo de activos de información y, por lo tanto, causen daños a una organización

Conflictos de interés: cuando el interés general propio de la función pública entra en conflicto con el interés particular y directo del servidor público".

Defensa jurídica: situaciones administrativas, jurídicas o de cualquier índole que generan litigiosidad e implica el uso de recursos públicos para reducir los eventos generadores del daño

Riesgo LA/FT: posibilidad de pérdida o daño por la propensión de la entidad a ser utilizada directa o a través de sus operaciones, como instrumento para cometer delitos de LA (Lavado de Activos), o canalización de recursos para la FT (Financiación del Terrorismo). Dentro de los cuales se encuentran:

- Riesgo reputacional: es la posibilidad de pérdida, disminución de ingresos o incremento en procesos judiciales en que incurre una entidad vigilada a causa de desprestigio, mala imagen, publicidad negativa respecto de la institución y sus prácticas de negocios.

- Riesgo legal: es la posibilidad de pérdida en que incurre una entidad a causa de sanciones o indemnizaciones de daños como resultado del incumplimiento normativo o de obligaciones contractuales. Se presenta de igual forma cuando existen fallas en los contratos y transacciones por actuaciones, negligencia o actos involuntarios.

- Riesgo operativo: es la posibilidad de pérdida en que incurre una entidad a causa de fallas, deficiencias o inadecuaciones en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de eventos externos.

- Riesgo de contagio: es la posibilidad de pérdida en que incurre una entidad por una acción o experiencia de un vinculado, entendido este como el relacionado o asociado, incluyendo a las personas naturales y/o jurídicas que ejercen influencia sobre la entidad.

RESPONSABILIDAD DE LA GESTIÓN DEL RIESGO Y CONTROL

La responsabilidad frente a la gestión del riesgo está definida mediante las líneas de defensa, así:

LINEA DE DEFENSA	RESPONSABLE	RESPONSABILIDAD DE LA GESTION DEL RIESGO Y CONTROL
ESTRATÉGICA	**Alta Dirección** **Comité Institucional de Coordinación de Control Interno.** **Comité Institucional de Gestión y desempeño**	• Definir el marco general para la gestión del riesgo y el control, supervisión del cumplimiento • Establecer y aprobar la política de riesgo. • Análisis de eventos y riesgos críticos • Definir y hacer seguimiento a los niveles de aceptación (apetito del riesgo) • Analizar los cambios del entorno que tengan impacto significativo en la operación de la entidad y que puedan generar cambios en la estructura de riesgos y controles • Realizar seguimiento a los riesgos institucionales • Liderar la implementación de la política • Evaluar el estado del control interno
PRIMERA DEFENSA	**Líderes de procesos y sus equipos** **Subdirector(a) de Salud Integral a la Fauna** **Subdirector(a) de Gestión del conocimiento y Cultura Ciudadana** **Subdirector de Gestión Corporativa** **Jefe Oficina Asesora Jurídica** **Jefe Oficina Asesora de Planeación**	• Responsables de gestionar el riesgo • Desarrollar e implementar procesos de control y gestión de riesgos a través de su identificación, análisis valoración, monitoreo y acciones de mejora • Monitorear y revisar periódicamente la gestión del riesgo y si es el caso ajustarla • Identificar y/o actualizar los riesgos y controles de procesos y proyectos a cargo, teniendo en cuenta los cambios del entorno y nuevas amenazas. • Realizar seguimiento a los controles para mitigar los riesgos según periodicidad establecida y proponer mejoras a la gestión de este. • Supervisar la ejecución de los controles aplicados por el equipo de trabajo • Desarrollar ejercicios de autoevaluación para establecer la eficiencia, eficacia y efectividad de los controles • Informar a la Oficina Asesora de Planeación (segunda línea) sobre los riesgos materializados en los programas, proyectos y procesos a cargo
SEGUNDA DEFENSA	**Oficina Asesora de Planeación**	• Capacita y acompaña en la metodología • Asegura que los controles y los procesos de gestión de riesgo implementados por la primera línea de defensa, estén diseñados apropiadamente y funcionen como se pretende • Asesorar a la línea estratégica en el análisis del contexto interno y externo • Acompañar y orientar sobre la metodología para la identificación, análisis, calificación y valoración del riesgo. • Consolidar el Mapa de riesgos institucional • Adelantar el monitoreo de la gestión del riesgo y la efectividad de los controles establecidos. • Acompañar, orientar y entrenar a los líderes de los procesos en lo que respecta a la metodología

LINEA DE DEFENSA	RESPONSABLE	RESPONSABILIDAD DE LA GESTION DEL RIESGO Y CONTROL
		• Evaluar la coherencia de los mapas presentados por los procesos, con lo que requiere la metodología aplicada. • Monitorear cambio de entorno y nuevas amenazas de la entidad.
TERCERA DEFENSA	**Oficina de Control Interno**	• Proporcionar información sobre la efectividad del SCI a través de un enfoque basado en riesgos incluida la operación de la primera y segunda línea de defensa • Proporcionar aseguramiento objetivo sobre la eficacia de la gestión del riesgo y el control • Asesorar en forma coordinada con la Oficina Asesora de planeación a la primera línea de defensa en la identificación de los riesgos institucionales y el diseño de controles. • Llevar a cabo el seguimiento a los riesgos de acuerdo con el Plan anual de auditoria y el seguimiento programado. • Reportar seguimiento de los riesgos del Instituto a la alta dirección.

El Instituto de Protección y Bienestar Animal en atención a las responsabilidades por línea de defensa comunica la información relevante hacia el interior de la entidad, respecto a la gestión del riesgo, así como a los grupos de valor y partes interesadas relacionadas con: actualización de la Política de Administración del Riesgo, cambios en el entorno y resultados del monitoreo, seguimiento y evaluación de riesgos, toda vez que entre otras actividades, se debe comunicar y consultar con los interesados internos y externos según corresponda en cada etapa del proceso de administración de riesgos.

IDENTIFICACIÓN DEL RIESGO

Identificar los riesgos de gestión y/o conflictos de interés que estén o no bajo el control del Instituto, para ello se debe tener en cuenta el contexto estratégico en el que opera la entidad, la caracterización de cada proceso que contempla su objetivo y alcance y, también, el análisis frente a los factores internos y externos que pueden generar riesgos que afecten el cumplimiento de los objetivos.

Con el fin de facilitar la identificación de riesgos de corrupción y evitar que se presenten confusiones entre un riesgo de gestión y uno de corrupción, se utilizara la **matriz de definición de riesgo de corrupción**, que incorpora cada uno de los componentes de su definición

	Marque con una X			
Descripción del riesgo	**Acción u omisión**	**Uso del poder**	**Desviar la gestión de lo publico**	**Beneficio privado**

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas V5

Para la gestión de la seguridad de la Información, la presente política se apoya en MSPI definido por el Ministerio de Tecnologías de la Información y las Comunicaciones, e integrado con el MGRSD para la gestión de riesgos.

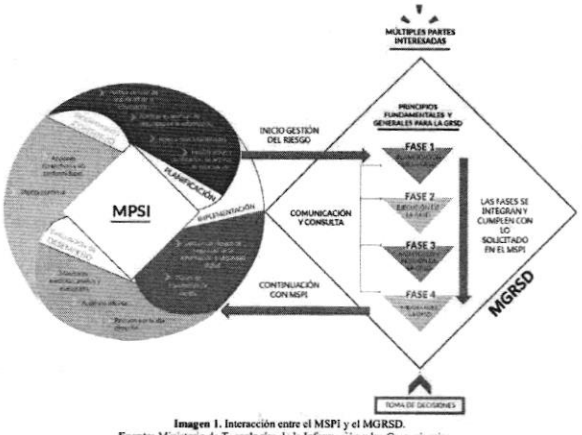


Imagen 1. Interacción entre el MSPI y el MGRSD.
Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones

Para la identificación de los riesgos de seguridad de la información es necesario identificar los activos de información del proceso. Se podrán identificar los siguientes tres (3) riesgos inherentes de seguridad de la información:

- Pérdida de la confidencialidad
- Pérdida de la integridad
- Pérdida de la disponibilidad

Para cada riesgo se deben asociar el grupo de activos, o activos específicos del proceso, y conjuntamente analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización.

Factores de riesgo

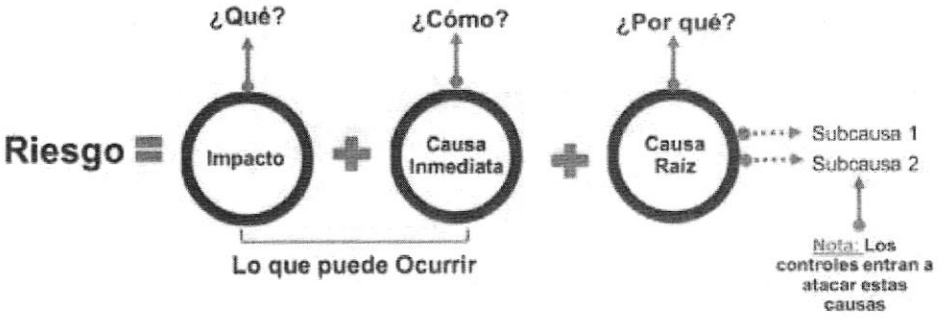
Factor	Definición	Descripción
Procesos	Eventos relacionados con errores en las actividades que deben realizar los servidores del Instituto	Falta de procedimientos Errores de grabación, autorización Errores en cálculos para pagos internos y externos Falta de capacitación, temas relacionados con el personal
Talento humano	Incluye seguridad y salud en el trabajo. Se analiza posible dolo e intención frente a la corrupción.	Hurtos activos Posibles comportamientos no éticos de los empleados Fraude interno (corrupción, soborno)
Tecnología	Eventos relacionados con la infraestructura tecnológica del Instituto	Daño de equipos Caída de aplicaciones Caída de redes Errores en programas
Infraestructura	Eventos relacionados con la infraestructura física de la entidad.	Derrumbes Incendios Inundaciones Daños a activos fijos
Evento externo	Situaciones externas que afectan la entidad.	Suplantación de identidad Asalto a la oficina Atentados, vandalismo, orden público

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas V5

Descripción del riesgo:

Debe contener todos los detalles que sean necesarios y que sea fácil de entender tanto para el líder del proceso como para personas ajenas al proceso. Se propone una estructura que facilita su redacción y claridad que inicia con la frase POSIBILIDAD DE y se analizan los siguientes aspectos:

Figura 10 Estructura propuesta para la redacción del riesgo



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas V5

Clasificación de riesgos

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

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas V5

VALORACIÓN DEL RIESGO

Determinar la probabilidad: se entiende como la posibilidad de ocurrencia del riesgo.

Actividad	Frecuencia de la Actividad	Probabilidad frente al Riesgo
Planeación estratégica	1 vez al año	Muy baja
Actividades de talento humano, jurídica, administrativa	Mensual	Media

Contabilidad, cartera	Semanal	Alta
*Tecnología (incluye disponibilidad de aplicativos), tesorería Misionalidad ***Nota:** En materia de tecnología se tiene en cuenta 1 hora funcionamiento = 1 vez. Ej.: Aplicativo FURAG está disponible durante 2 meses las 24 horas, en consecuencia, su frecuencia se calcularía 60 días * 24 horas= 1440 horas.	Diaria	Muy alta

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas V5

Nivel de probabilidad: la exposición al riesgo estará asociada al proceso o actividad que se esté analizando, es decir, al número de veces que se pasa por el punto de riesgo en el periodo de 1 año. Para determinar la probabilidad de los riesgos de seguridad de la información se determina con base a la amenaza no en las vulnerabilidades

	Frecuencia de la Actividad	Probabilidad
Muy Baja	La actividad que con lleva el riesgo se ejecuta como máximos 2 veces por año	20%
Baja	La actividad que con lleva el riesgo se ejecuta de 3 a 24 veces por año	40%
Media	La actividad que con lleva el riesgo se ejecuta de 24 a 500 veces por año	60%
Alta	La actividad que con lleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5000 veces por año	80%
Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año	100%

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas V5

Para los riesgos de corrupción se analiza qué tan posible es que ocurra el riesgo, se expresa en términos de frecuencia o factibilidad, donde frecuencia implica analizar el número de eventos en un periodo determinado, se trata de hechos que se han materializado o se cuenta con un historial de situaciones o eventos asociados al riesgo, los criterios para calificar la probabilidad son:

Nivel	Descriptor	Descripción	Frecuencia
5	Casi Seguro	Se espera que el evento ocurra en la mayoría de las circunstancias	Mas 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 año
3	Posible	El evento podrá ocurrir en algún momento	Al menos 1 vez en los últimos dos 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 V5

Nivel de Impacto: Para la construcción de la tabla de criterios se definen los impactos económicos y reputacionales como las variables principales.
Cuando se presenten ambos impactos para un riesgo, tanto económico como reputacional, con diferentes niveles se debe tomar el nivel más alto.

	Afectación Económica	Reputacional
Leve 20%	Afectación menor a 10 SMLMV.	El riesgo afecta la imagen de algún área del Instituto

Menor 40%	Entre 10 y 50 SMLMV	El riesgo afecta la imagen del Instituto internamente, de conocimiento general nivel interno, de junta directiva y proveedores.
Moderado 60%	Entre 50 y 100 SMLMV	El riesgo afecta la imagen del Instituto con algunos usuarios de relevancia frente al logro de los objetivos.
Mayor 80%	Entre 100 y 500 SMLMV	El riesgo afecta la imagen del Instituto con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal.
Catastrófico 100%	Mayor a 500 SMLMV	El riesgo afecta la imagen del Instituto a nivel nacional, con efecto publicitario sostenido a nivel país

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas V5

Para determinar el impacto de los riesgos de seguridad de la información se determina con base a la amenaza no en las vulnerabilidades. Se debe definir el posible origen del riesgo de la seguridad de la información. Por debilidades en Hardware, Software, Red, Personal, Lugar y Otros. Se selecciona de una lista desplegable el posible origen del riesgo:

TABLA DE VULNERABILIDADES
Seleccionar Vulnerabilidad
Hardware: Mantenimiento insuficiente
Hardware: Ausencia de esquemas de reemplazo periódico
Hardware: Sensibilidad a la radiación electromagnética
Hardware: Susceptibilidad a las variaciones de temperatura (o al polvo y suciedad)
Hardware: Almacenamiento sin protección
Hardware: Falta de cuidado en la disposición final
Hardware: Copia no controlada
Software: Ausencia o insuficiencia de pruebas de software
Software: Ausencia de terminación de sesión
Software: Ausencia de registros de auditoría
Software: Asignación errada de los derechos de acceso
Software: Interfaz de usuario compleja
Software: Ausencia de documentación
Software: Fechas incorrectas
Software: Ausencia de mecanismos de identificación y autenticación de usuarios
Software: Contraseñas sin protección
Software: Software nuevo o inmaduro
Red: Ausencia de pruebas de envío o recepción de mensajes
Red: Líneas de comunicación sin protección
Red: Conexión deficiente de cableado
Red: Tráfico sensible sin protección
Red: Punto único de falla
Personal: Ausencia del personal

Personal: Entrenamiento insuficiente
Personal: Falta de conciencia en seguridad
Personal: Ausencia de políticas de uso aceptable
Personal: Trabajo no supervisado de personal externo o de limpieza
Lugar: Uso inadecuado de los controles de acceso al edificio
Lugar: Áreas susceptibles a inundación
Lugar: Red eléctrica inestable
Lugar: Ausencia de protección en puertas o ventanas
Organización: Ausencia de procedimiento de registro/retiro de usuarios
Organización: Ausencia de proceso para supervisión de derechos de acceso
Organización: Ausencia de control de los activos que se encuentran fuera de las instalaciones
Organización: Ausencia de acuerdos de nivel de servicio (ANS o SLA)
Organización: Ausencia de mecanismos de monitoreo para brechas en la seguridad
Organización: Ausencia de procedimientos y/o de políticas en general (esto aplica para muchas actividades que la entidad no tenga documentadas y formalizadas como uso aceptable de activos, control de cambios, valoración de riesgos, escritorio y pantalla limpia entre otros)

Para los riesgos de corrupción el impacto se debe analizar y calificar a partir de las consecuencias identificadas en la fase de descripción del riesgo así:

No	Pregunta: Si el riesgo de Corrupción se materializa se podría...	Respuesta	
		Si	No
1	¿Afectar al grupo de funcionarios del proceso?		
2	¿Afectar el cumplimiento de metas y objetivos de las dependencias?		
3	¿Afectar el cumplimiento de la misión del Instituto?		
4	¿Afectar el cumplimiento de la misión del sector al que pertenece el Instituto?		
5	¿Generar perdidas de confianza del Instituto, afectando su reputación?		
6	¿Generar perdidas de recursos económicos?		
7	¿Afectar la prestación de servicios?		
8	¿Dar lugar al detrimento de calidad de vida de la comunidad por perdida del bien, servicios o recursos públicos?		
9	Generar perdida de información del Instituto		
10	¿Generar intervención de los entes 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 pérdidas de vidas humanas?		
17	¿Afectar la imagen regional?		
18	¿Afectar la imagen nacional?		
19	¿Generar daño ambiental?		

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas V5

Responder afirmativamente de 1 a 5 preguntas genera un impacto MODERADO

Responder afirmativamente de 6 a 11 preguntas genera un impacto MAYOR
Responder afirmativamente de 12 a 19 preguntas genera un impacto CATASTROFICO

MODERADO	genera medianas consecuencias al Instituto
MAYOR	genera altas consecuencias al Instituto
CATASTROFICO	genera consecuencias desastrosas para el Instituto

Nota: si la respuesta a la pregunta 16 es afirmativa el riesgo se considera CATASTROFICO

EVALUACIÓN DE RIESGOS: a partir del análisis de la probabilidad de ocurrencia del riesgo y sus consecuencias o impactos, se busca determinar la zona de riesgo inicial (RIESGO INHERENTE).

Matriz de Calor

Probabilidad	Impacto				
	Leve 20%	Menor 40%	Moderado 60%	Mayor 80%	Catastrófico 100%
Muy alta 100%	A	A	A	A	E
Alta 80%	M	M	A	A	E
Media 60%	M	M	M	A	E
Baja 40%	B	B	M	A	E
Muy baja 20%	B	B	M	A	E
B: Zona de riesgo **baja** M: Zona de Riesgo **moderada** A: Zona de Riesgo **Alta** E: Zona de Riesgo **Extrema**					

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas V5

Para los riesgos de corrupción, se tendrá en cuenta la siguiente matriz de calor, el análisis de impacto se realizará teniendo en cuenta solamente los niveles "moderado", "mayor" y "catastrófico", dado que estos riesgos siempre serán significativos; en este orden de ideas, no aplican los niveles de impacto insignificante y menor, que sí aplican para los demás riesgos.

Probabilidad	Impacto				
	Insignificante (1)	Menor (2)	Moderado (3)	Mayor (4)	Catastrófico (5)
Casi Seguro (1)	NA	NA	E	E	E
Probable (2)	NA	NA	A	E	E
Posible (3)	NA	NA	A	E	E
Improbable (4)	NA	NA	M	A	E
Rara Vez (1)	NA	NA	M	A	E
M: Zona de Riesgo moderada A: Zona de Riesgo Alta E: Zona de Riesgo Extrema					

Definición de controles: para una adecuada redacción del control se propone una estructura que facilitará más adelante entender su tipología y otros atributos para su valoración. La estructura es la siguiente:

- **Responsable de ejecutar el control:** identificar el cargo del servidor que ejecuta el control, en caso de que sean controles automáticos se identificará el sistema que realiza la actividad.
- **Acción:** se determinará mediante verbos que indican la acción que deben realizar como parte del control.
- **Complemento**: corresponde a los detalles que permiten identificar claramente el objeto del control.

Tipologías de controles

- **Control preventivo:** control accionado en la entrada del proceso y antes de que se realice la actividad originadora del riesgo, se busca establecer las condiciones que aseguren el resultado final esperado, va a las causas del riesgo, ataca la probabilidad de ocurrencia del riesgo. (atacan probabilidad)
- **Control detectivo:** control accionado durante la ejecución del proceso. Estos controles detectan el riesgo, pero generan reprocesos. Detecta que algo ocurre y devuelve el proceso a los controles preventivos Atacan la probabilidad de ocurrencia del riesgo. (atacan probabilidad)
- **Control correctivo:** control accionado en la salida del proceso y después de que se materializa el riesgo. Estos controles tienen costos implícitos. Atacan el impacto frente a la materialización del riesgo. (atacan impacto)

Así mismo, de acuerdo con la forma como se ejecutan tenemos:

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

Atributos para el diseño del control

Características	Descripción			Peso
Atributos de eficiencia	Tipo	Preventivo	Va hacia las causas del riesgo, aseguran el resultado final esperado.	**25%**
		Detectivo	Detecta que algo ocurre y devuelve el proceso a los controles preventivos. Se pueden generar reprocesos.	**15%**
		Correctivo	Dado que permiten reducir el impacto de la materialización del riesgo, tienen un costo en su implementación.	**10%**

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

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas V5

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

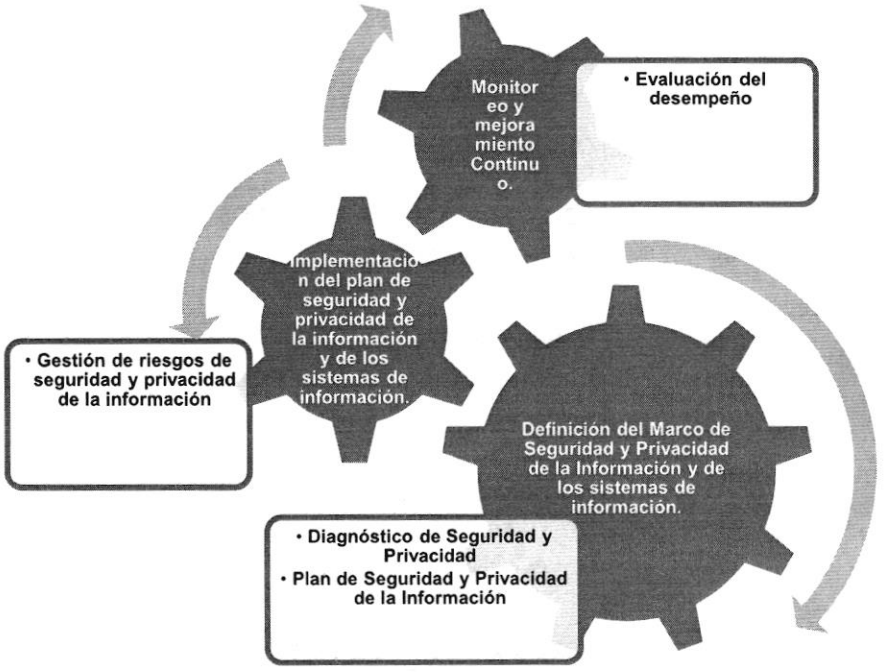
El desplazamiento del riesgo inherente de corrupción para calcular el riesgo residual únicamente hay disminución de probabilidad, es decir para el impacto no opera el desplazamiento.

Para la selección de controles que permitan disminuir la probabilidad o el impacto del riesgo de seguridad de la información, nos basamos en la norma ISO/IEC 27001:2013 en su Anexo A, como un insumo base para mitigar los riesgos.
Estos controles se organizados por dominios, como se muestran a continuación.

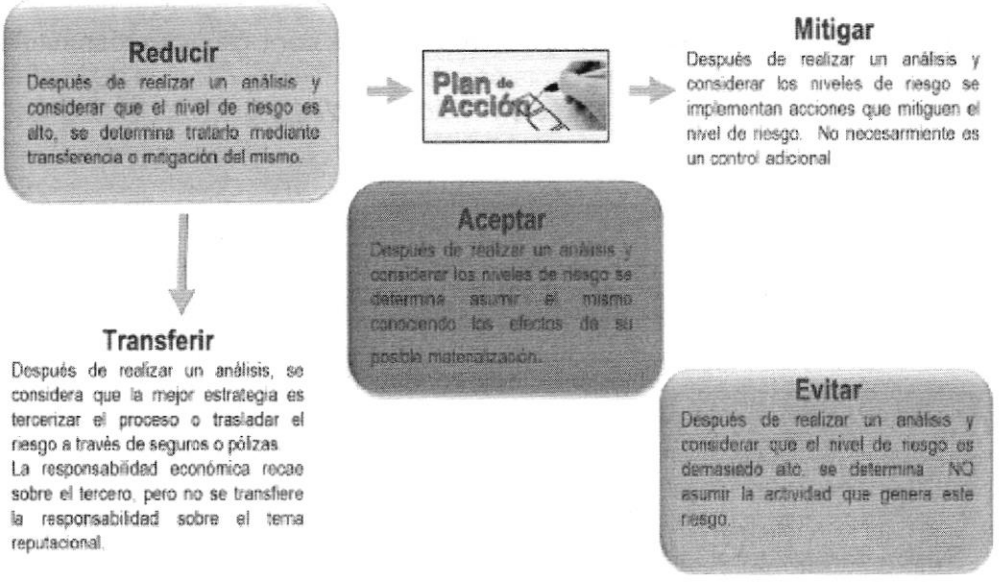
DOMINIO	DESCRIPCIÓN
A5	POLÍTICAS DE LA SEGURIDAD DE LA INFORMACION
A6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACION
A7	SEGURIDAD DE LOS RECURSOS HUMANOS
A8	GESTION DE ACTIVOS
A9	CONTROL DE ACCESO
A10	CRIPTOGRAFIA
A11	SEGURIDAD FISICA Y DEL ENTORNO
A12	SEGURIDAD DE LAS OPERACIONES
A13	SEGURIDAD DE LAS COMUNICACIONES
A14	ADQUISICION, DESARROLLO Y MANTENIMIENTO DE SISTEMAS
A15	RELACIONES CON LOS PROVEEDORES
A16	GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION
A17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTION DE CONTINUIDAD DE NEGOCIO
A18	CUMPLIMIENTO

Controles de referencia para la mitigación de riesgos de seguridad de acuerdo con el Anexo A del ISO 27001:2013

Una vez realizada la valoración de los riesgos y establecidos los controles con respecto a la seguridad de la información, se debe establecer los mecanismos de seguimiento y control de la efectividad en los controles, a través de un ciclo continuo de mejora (Ciclo PHVA), como se muestra en la siguiente gráfica.



Estrategias para combatir el riesgo: decisión que se toma frente a un determinado nivel de riesgo, dicha decisión puede ser aceptar, reducir o evitar. Se analiza frente al riesgo residual, esto para procesos en funcionamiento, cuando se trate de procesos nuevos, se procede a partir del riesgo inherente.



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas V5

Para el caso de los riesgos de corrupción estos no pueden ser "Aceptados"

Para el caso de los riesgos de seguridad de la información se podrán "mitigar/tratar"

SISTEMA DE ADMINISTRACIÓN DE RIESGOS DE LAVADO DE ACTIVOS Y DE LA FINANCIACIÓN DEL TERRORISMO

TÉRMINOS O DEFINICIONES

Colocación: consiste en la recepción física de bienes de cualquier naturaleza o de dinero, en desarrollo y como consecuencia de actividades ilícitas que pretenden ser puestas en el sistema económico.

Transformación, Ocultamiento: consiste en la introducción de los fondos (dinero físico) o bienes, en la economía legal, seguida de sucesivas operaciones (nacionales o internacionales), para ocultar, invertir, o para mezclarlos con dinero de origen legal, con el fin de disimular su origen.

Integración: en este paso, el dinero lavado regresa a la economía disfrazado ahora como "dinero legítimo".

Medidas de prevención y gestión del riesgo de LA/FT: Es necesario realizar una medición de los riesgos LAFT y el establecimiento de controles para mitigar la consecución de dichos riesgos.

Sistema de Administración de Riesgo SARLAFT: El Sistema de Administración de Riesgos- SARLAFT comprende todas las actividades a ser realizadas por la Entidad en desarrollo de su objeto social principal y deberá contener, adicionalmente, los procedimientos y metodologías para que esté protegida de ser utilizada en forma directa, es decir a través de sus administradores, vinculados o contrapartes, como instrumento para el lavado de activos, ocultamiento de activos provenientes de dichas actividades y/o canalización de recursos hacia la financiación de actividades terroristas.

El Sistema de Administración de Riesgos- SARLAFT comprende todas las actividades a ser realizadas por la Entidad en desarrollo de su objeto social principal y deberá contener, adicionalmente, los procedimientos y metodologías para que esté protegida de ser utilizada en forma directa, es decir a través de sus administradores, vinculados o contrapartes, como instrumento para el lavado de activos, ocultamiento de activos provenientes de dichas actividades y/o canalización de recursos hacia la financiación de actividades terroristas[1]

La Secretaría General de la Alcaldía Mayor de Bogotá presentó el documento Ruta Metodológica para la Implementación del SARLAFT en las Entidades Distritales, en el cual señala los pasos para la integración y los elementos del sistema de gestión del riesgo, resumidos en lo siguiente:

No.	Paso	Descripción
1.	Identificación de los riesgos de LA/FT	Para la identificación del riesgo el marco de referencia es la metodología establecida por el Departamento Administrativo de la Función Pública, y los riesgos identificados serán incorporados en la matriz de riesgo del Instituto. Se revisarán las herramientas presentadas por el documento antes citado para el ejercicio de identificación (Cuestionario de autoevaluación del riesgo operativo y el Cuestionario de autoevaluación sobre el control del riesgo de LA/FT).

[1] Lineamiento Para Prevenir el lavado de Activos y contra la Financiación del Terrorismo en las Entidades Distritales Tomo I – Dirección De Desarrollo Institucional de la Secretaría General de la Alcaldía Mayor de Bogotá

2.	Medir el riesgo de LA/FT	Para la medición se tendrán en cuenta las escalas de probabilidad e impacto utilizando las tablas de clasificación definidas en esta política, teniendo en cuenta el alcance del objetivo respecto a los temas de LA/FT y comprendiendo que a mayor exposición al riesgo de LA/FT mayor será el impacto para la entidad, esto conlleva a determinar los eventos críticos.
3.	Controlar el riesgo de LA/FT	**CONTROL PREVENTIVO** Tiene como objetivo evitar que se introduzcan recursos de actividades ilícitas a través de la entidad, identificando la fuente del riesgo y quien lo genera, para fortalecer el esquema de prevención. **CONTROL DETECTIVO** Su finalidad es identificar señales de alerta que se generan por un número de hechos que sumados se salen del normal desarrollo económico y se convierte en una operación inusual, que debe ser evaluada para determinar su reporte como una operación sospechosa de UIAF.
4.	Monitorear el riesgo de LA/FT	Se centra en determinar la efectividad y oportunidad de los controles implementados en el sistema SARLAFT respecto del tratamiento de los riesgos, y se realiza en armonía con la actividad de monitoreo establecida en la estructura MECI1, respecto del control y vigilancia del riesgo y planteado también en la guía mencionada del DAFP dentro de las líneas estratégicas de defensa relacionadas. **Primera línea de defensa:** gestión operativa **Segunda línea de defensa:** funciones de gestión de riesgo y cumplimiento **Tercera línea de defensa:** auditoría interna

Fuente: Lineamiento Para Prevenir el lavado de Activos y contra la Financiación del Terrorismo en las Entidades Distritales Tomo I – Dirección De Desarrollo Institucional de la Secretaría General de la Alcaldía Mayor de Bogotá