PRESENTACIÓN

El concepto de Administración del Riesgo se introduce en las entidades públicas, teniendo en cuenta que todas las organizaciones independientemente de su naturaleza, tamaño y razón de ser, están permanentemente expuestas a diferentes riesgos o eventos que afectan el logro de objetivos institucionales.

Con la implementación del Modelo Integrado de Planeación y Gestión-MIPG, a través de la política de Planeación Institucional correspondiente a la Dimensión de Direccionamiento Estratégico, de acuerdo con su plataforma estratégica, el esquema de procesos, procedimientos, políticas de operación, sistemas de información, tendrá insumos esenciales para iniciar con la aplicación de la metodología propuesta para la administración del riesgo. Este enfoque toma como base el documento "Guía para la administración del riesgo y el diseño de controles en entidades públicas" emitido por el Departamento Administrativo de la Función Pública en el año 2020; por la NTC-ISO 31000 e ISO 9001:2015, que destacan la metodología como una herramienta preventiva.

Así mismo, de acuerdo con los lineamientos de COSO 2013 y COSO ERM 2017, los planes, programas o proyectos deben contemplar los riesgos para su ejecución y logro de sus objetivos.

Con este marco la ESE Hospital Local Cartagena de Indias, ha elaborado el presente Manual para la Administración del Riesgo, a través del cual establece los lineamientos para la identificación, análisis, valoración, evaluación, tratamiento, respuesta a los riesgos y escenario 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, Guía para la Administración del Riesgo y el Diseño de Controles en entidades Públicas y el Modelo de Seguridad y Privacidad de la Información de la estrategia de Gobierno Digital.

1. OBJETIVO GENERAL

Establecer una guía metodológica que facilite la comprensión e implementación de la administración del riesgo en la ESE HLCI, brindando lineamientos para la identificación, análisis, valoración de riesgos, monitoreo y revisión, determinación de roles y responsabilidades (esquema de líneas de defensa), 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 de respuesta a eventos identificados que afecten al Talento Humano, la Infraestructura Tecnológica o los servicios esenciales de los que depende la ESE HLCI.

1.1. OBJETIVOS ESPECÍFICOS

Proteger los recursos de la Entidad, resguardándolos contra la materialización de los riesgos valorados como amenazas de corrupción, de seguridad digital o de gestión.

Involucrar y comprometer a todos los servidores de la Entidad en la búsqueda de acciones encaminadas a gestionar los riesgos de los procesos en los cuales participa.

Suministrar lineamientos basados en una adecuada gestión del riesgo y control a los mismos, que permitan a la Entidad, tener una seguridad razonable en el logro de sus objetivos, bajo el cumplimiento de normas, leyes y regulaciones aplicables.

Ofrecer herramientas para identificar, analizar, evaluar los riesgos y determinar roles y responsabilidades de cada uno de los servidores y/o colaboradores de la Entidad.

2. ALCANCE

Aplica a todos los proyectos, servicios, procesos, planes, programas, de la Entidad y a todas las actividades ejecutadas por los servidores públicos en el ejercicio de sus funciones para la gestión y control de los riesgos de gestión, corrupción y seguridad digital de la Entidad.

3. BASE LEGAL

Ley 87 de 1993. Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del Estado y se dictan otras disposiciones.

Directiva presidencial 09 de 1999. Lineamientos para la implementación de la política de lucha contra la corrupción.

Ley 1474 de 2011. Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.

Decreto 4170 de 2011. Por el cual se crea la Agencia Nacional de Contratación Pública –Colombia Compra Eficiente–, se establece la necesidad de "crear políticas unificadas que sirvan de guía a los administradores de compras y que permitan monitorear y evaluar el desempeño del sistema y generar mayor transparencia en las compras".

NTC ISO 9001: 2015. Requisitos Sistema de Gestión de Calidad.

Decreto 1083 de 2015. "Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública".

Decreto 648 de 2017. Por el cual se modifica y adiciona el Decreto 1083 de 2015, Reglamentario Único del Sector de la Función Pública.

Decreto 1499 de 2017. Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.

Norma ISO/IEC 27001. Lineamientos para la gestión de seguridad y privacidad de la información.

NTC ISO 31000:2018. Lineamientos Administración / Gestión de riesgos.

Decreto 1008 de 2018. Establece lineamientos generales de la Política de Gobierno Digital para Colombia, antes estrategia de Gobierno en Línea, la cual desde ahora debe ser entendida como: el uso y aprovechamiento de las tecnologías de la información y las comunicaciones para consolidar un Estado y ciudadanos competitivos, proactivos, e innovadores, que generen valor público en un entorno de confianza digital.

Decreto 2106 de 2019. Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública".

Manual Operativo del Modelo Integrado de Planeación y Gestión Versión 4.

Guía para la Administración del Riesgo en la Gestión, Corrupción y Seguridad Digital. Diseño de Controles en Entidades Públicas Versión 5 de Noviembre de 2020.

Guía de orientación de aplicación de la GRSD en el sector público, territoriales y gobierno nacional.

Guía "Estrategias para la Construcción del Plan Anticorrupción y de Atención al Ciudadano" de la Secretaria de Transparencia de la Presidencia de la República.

4. DEFINICIONES

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 de Riesgo: Es el nivel de riesgo que la entidad puede aceptar, relacionado con sus objetivos, el marco legal y las disposiciones de la Alta Dirección y del Órgano de Gobierno. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.

Capacidad del Riesgo: Es el máximo valor del nivel de riesgo que una entidad puede soportar y a partir del cual se considera por la Alta Dirección y el Órgano de Gobierno que no sería posible el logro de los objetivos de la Entidad.

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.

Confidencialidad. Propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados.

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.

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.

CGDI. Comité de Gestión y Desempeño Institucional.

CICCI. Comité Institucional de Coordinación de Control Interno.

Disponibilidad. Propiedad de ser accesible y utilizable a demanda por una entidad.

Factores de Riesgo. Son las fuentes generadoras de riesgos.

Fraude. Acción de engaño intencional, que un servidor público o particular con funciones, públicas, realiza con el propósito de conseguir un beneficio o ventaja ilegal para sí mismo o para un tercero.

Gestión del Riesgo. Proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos.

Impacto. Las consecuencias que puede ocasionar a la organización la materialización del riesgo.

Integridad. Propiedad de exactitud y completitud

Mapa de Riesgos. Documento que resume los resultados de las actividades de gestión de riesgos, incluye una presentación 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.

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 un (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.

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 Operativo. Posibilidad de incurrir en pérdidas por errores, fallas o deficiencias en el Talento Humano, procesos, tecnologías, infraestructura y eventos externos.

Riesgo Residual. El resultado de aplicar la efectividad de los controles al riesgo inherente.

Riego de Seguridad Digital. Efecto que se causa sobre los objetivos de las entidades, debido a amenazas y vulnerabilidades en el entorno digital.

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 ISO 27000.

SGI. Sistema de Gestión Institucional.

TIC. Tecnologías de la Información y las Comunicaciones.

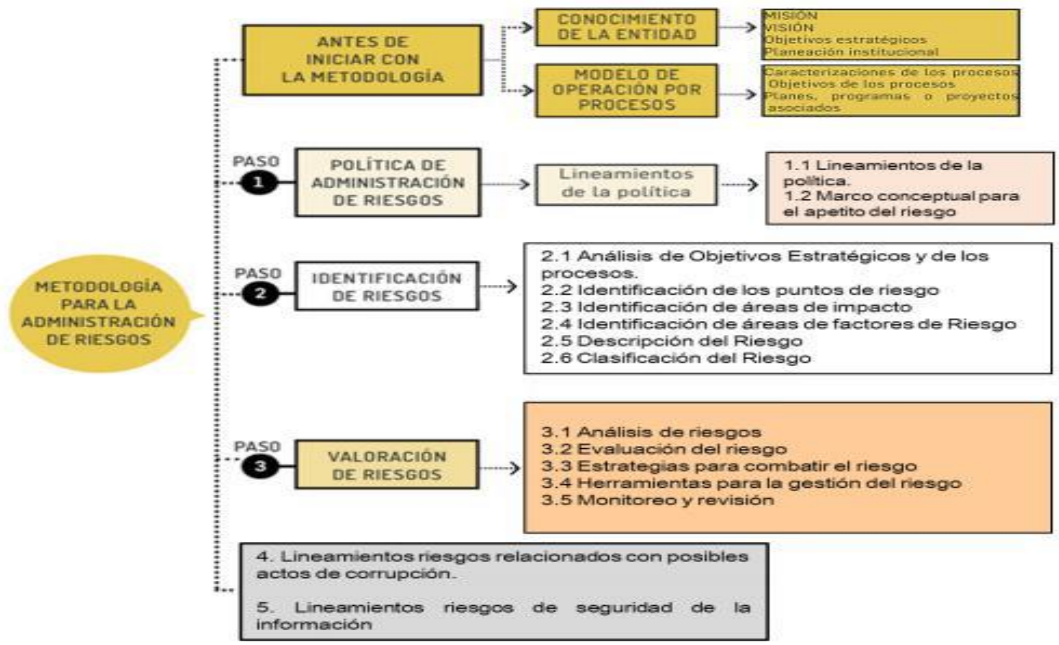
Tolerancia del Riesgo. Es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del apetito de riesgo determinado por la entidad.

Vulnerabilidad. Representa la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.

5. METODOLOGÍA PARA LA ADMINISTRACIÓN DEL RIESGO

El adecuado manejo de los riesgos favorece el desarrollo y crecimiento de la entidad, con el fin de asegurar dicho manejo es importante que se establezca el entorno y ambiente organizacional, la identificación, análisis, valoración y definición de las alternativas de acciones de mitigación de los riesgos, mediante el desarrollo de los siguientes elementos, que se ilustran a continuación en la gráfico1.

Gráfico 1

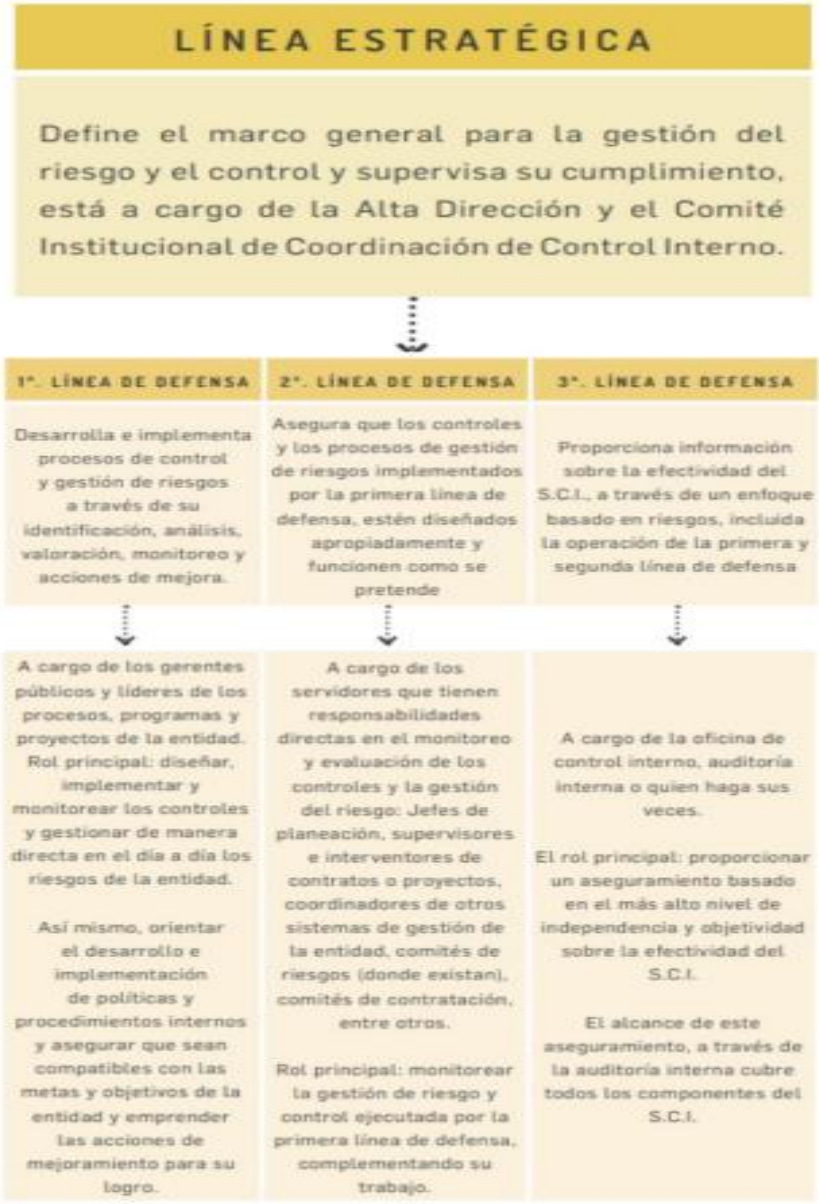


Fuente: Gráfico tomado y adaptado de Función pública. Guía para la administración del riesgo y el diseño de controles en entidades públicas Riesgos de gestión, corrupción y seguridad digital, Versión 5, 2020.

6. ROLES Y RESPONSABILIDADES

Los roles y responsabilidades en la gestión del riesgo son de carácter integral y diferenciado, donde participan todos los niveles de la gestión institucional, de esta manera se asegura el logro, anticipándose y minimizando los riesgos que pueden afectar a la entidad. Esta gestión se desarrolla a través de las líneas de defensa estratégica y de responsabilidad de la gestión del riesgo y control.

Gráfico 2
Esquema de Líneas de Defensa



Fuente: Dirección de Gestión y Desempeño Institucional de Función Pública, 2018.

7. POLÍTICA DE ADMINISTRACIÓN DE RIESGOS

Tabla 1
Lineamientos de la Política de Riesgos

¿Qué es?	¿Quién la Establece?	¿Qué se debe tener en cuenta?	¿Qué debe Contener?
La política de riesgos establece lineamientos precisos acerca del tratamiento, manejo y seguimiento a los riesgos. Es aplicable a todos los procesos, proyectos, planes de la Entidad y a las actividades ejecutadas por los servidores durante el ejercicio de sus funciones.	La establece la Alta Dirección de la Entidad, en el marco del Comité Institucional de Coordinación de Control Interno.	Los objetivos estratégicos de la Entidad. Nivel de responsabilidad frente al manejo de los riesgos. Mecanismos de comunicación para darla a conocer a todos los niveles de la Entidad.	Objetivo Alcance Niveles de aceptación del riesgo. Niveles para calificar el impacto. Tratamiento de riesgos. Periodicidad para el seguimiento de acuerdo con el nivel de riesgo residual. Responsables del seguimiento.

Fuente: Dirección de Gestión y Desempeño Institucional de Función Pública, 2018.

8. TIPOLOGÍA, FACTORES Y CLASIFICACIÓN DE RIESGOS

Con la finalidad de mantener una terminología común para las actividades de gestión de riesgos, la ESE Hospital Local Cartagena de Indias, establece la tipología, factores y clasificación para los riesgos en la tabla 2 de la siguiente manera:

Tabla 2
Tipología, Factores y Clasificación de Riesgos

Tipología	Factores de Riesgo	Clasificación					
Riesgo Operativo	Talento Humano	Fraude Interno	Pérdidas debido a actos de fraude, actuaciones irregulares, comisión de hechos delictivos, infidelidades, abuso de confiamza apropiación indebida o incumplimiento de regulaciones legales o internas de la Entidad.	**Seguridad Digital** Combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la autoridad institucional, la integridad de la Entidad, incluye aspectos relacionados con el ambiente físico, digital y las personas.	**Continuidad del Negocio** Relacionado a la interrupción no deseada o escenarios que afecten la vida de las persona o bienes de la Entidad, interrumpiendo sus funciones críticas parcial o totalmente	**Grupos de Valor,Productos o Servicios y prácticas de la Entidad** Fallas negligentes o involuntarias de las obligaciones frente a los grupos de valor y que impiden satisfacer una obligación profesional frente a estos.	**Relaciones Laborales** Pérdidas que surge de acciones contrarias a las leyes o acuerdos de empleos, salud o seguridad, del pago de demandas por daños personales o de discriminación.
		Daño Antijurídico	Falencia administrativa que ocasiona litigiosidad y puede ser tanto una acción como una omisión de la Entidad en desarrollo de sus actividades.				
		Corrupción	Posibilidad de que por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.				
	Eventos Externos	Fraude Externo	Pérdida debido a actos de fraude, apropiación indebida o incumplimiento de leyes por un externo.				
		Proveedores	Originado por las carencias del servicio prestado por proveedores y empresas subcontratadas.				
	Procesos	Ejecución y Administración de Procesos	Pérdidas derivadas de errores en la ejecución y administración de los procesos.				
	Tecnología	Fallas Tecnológicas	Pérdidas derivadas por fallas en Hardw are Softw are, telecomunicaciones o interrupciones en los servicios básicos.				
	Infraestructura	Daños a Activos Físicos	Pérdidas por daños o extravíos de los activos físicos por desaatres naturales y otros eventos.				

Fuente: Adaptado del Curso Riesgo Operativo de la Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

9. IDENTIFICACIÓN DEL RIESGO

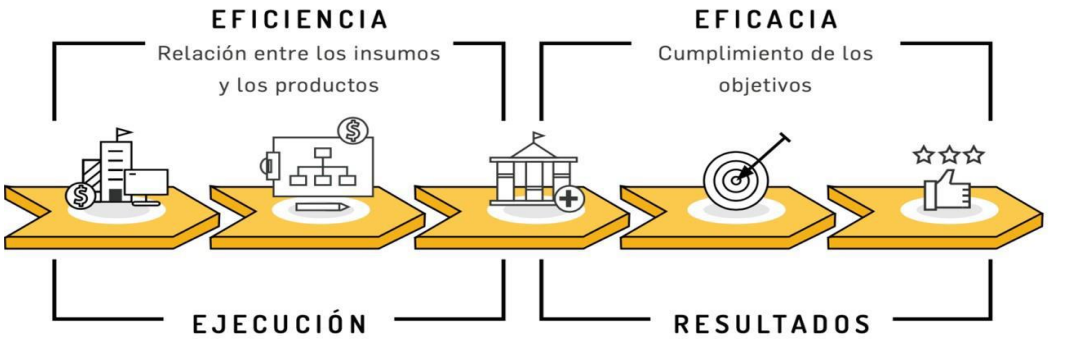
El objetivo es identificar los riesgos que estén o no bajo el control de la Entidad, para ello se debe tener en cuenta el contexto estratégico en el que opera la Entidad, la caracterización de cada proceso que contempla su objetivo y alcance, también, el análisis frente a los factores internos y externos que pueden generar riesgos que afecten el cumplimiento de los objetivos, aplicando las siguientes fases:

9.1. Análisis de Objetivos Estratégicos y de los Procesos. La Entidad debe analizar los objetivos estratégicos y revisar que se encuentren alineados con la misión y la visión institucional, así como su desdoble hacia los objetivos de los procesos. Se plantea la necesidad de analizar su adecuada formulación, es decir, que contengan unos atributos mínimos, para lo cual puede hacer uso de las características mínimas: específico, medible, alcanzable, relevante y proyectado.

9.2. Identificación de los Puntos de Riesgo. Dentro del flujo de los procesos identificados en la Entidad, existen actividades en las que se tienen evidencia o indicios de que pueden presentarse eventos de riesgo operativo, los cuales deben mantenerse controlados para asegurar que cada uno de los procesos cumpla con su objetivo y se garantice la cadena de valor.

Gráfico 3

CADENA DE VALOR PÚBLICO



Insumos	Procesos	Productos	Resultados o efectos	Impactos
Recursos financieros, humanos y materiales empleados para generar los productos.	Actividades realizadas para transformar los insumos en productos.	Bienes y servicios elaborados que requiere la población para satisfacer una demanda o dar respuesta a las causas concretas de un problema.	Cambios en el comportamiento o en el estado de los beneficiarios como consecuencia de recibir los productos (bienes o servicios).	Cambios en las condiciones de vida en la población objetivo. Mayor valor público en términos de bienestar, prosperidad general y calidad de vida de la población.

9.3 Identificación de Áreas de Impacto. El área de impacto es la consecuencia económica o reputacional a la cual se ve expuesta la organización en caso de materializarse un riesgo. Los impactos que aplican son afectación económica (o presupuestal) y reputacional.

9.4. Identificación de áreas de Factores de Riesgo. Son las fuentes generadoras de riesgos. En el Gráfico 4 encontrará un listado con ejemplo de factores de riesgo que puede tener una entidad.

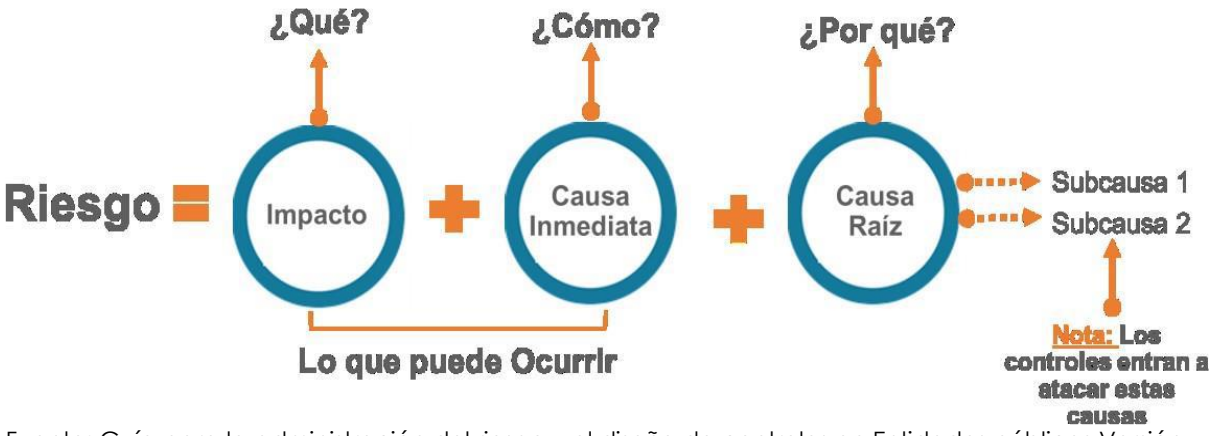
Gráfico 4
Identificación de áreas de Factores de Riesgo

Factor	Definición		Descripción
Procesos	Eventos relacionados con errores en las actividades que deben realizar los servidores de la Entidad		Falta de procedimientos
			Errores de grabación, autorización
			Errores en cálculos para pagos internos y externos.
			Falta de 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 de la Entidad.		Daño de equipos
			Caídas de aplicaciones
			Caídas 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 a 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 Versión 5 - diciembre de 2020

10. DESCRIPCIÓN DEL RIESGO. La descripción del riesgo debe contener todos los detalles que sean necesarios y que sea fácil de entender tanto para el líder del proceso, del equipo de trabajo y de cualquier persona ajena 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:

Gráfico 5
Estructura Propuesta para la Redacción del Riesgo



Fuente: Guía para la administración del riesgo y el diseño de controles en Entidades públicas Versión 5 - diciembre de 2020.

Desglosando la estructura propuesta se obtiene:

Impacto. Las consecuencias que puede ocasionar a la Entidad la materialización del riesgo.

Causa Inmediata. Circunstancias o situaciones más evidentes sobre las cuales se presenta el riesgo, las mismas no constituyen la causa principal o base para que se presente el riesgo.

Causa Raíz. Es la causa principal o básica, corresponden a las razones por la cuales se puede presentar el riesgo, son la base para la definición de controles en la etapa de valoración del riesgo. Se debe tener en cuenta que para un mismo riesgo pueden existir más de una causa o subcausas que pueden ser analizadas.

11. CLASIFICACIÓN DEL RIESGO. Los riesgos se clasifican con las siguientes categorías:

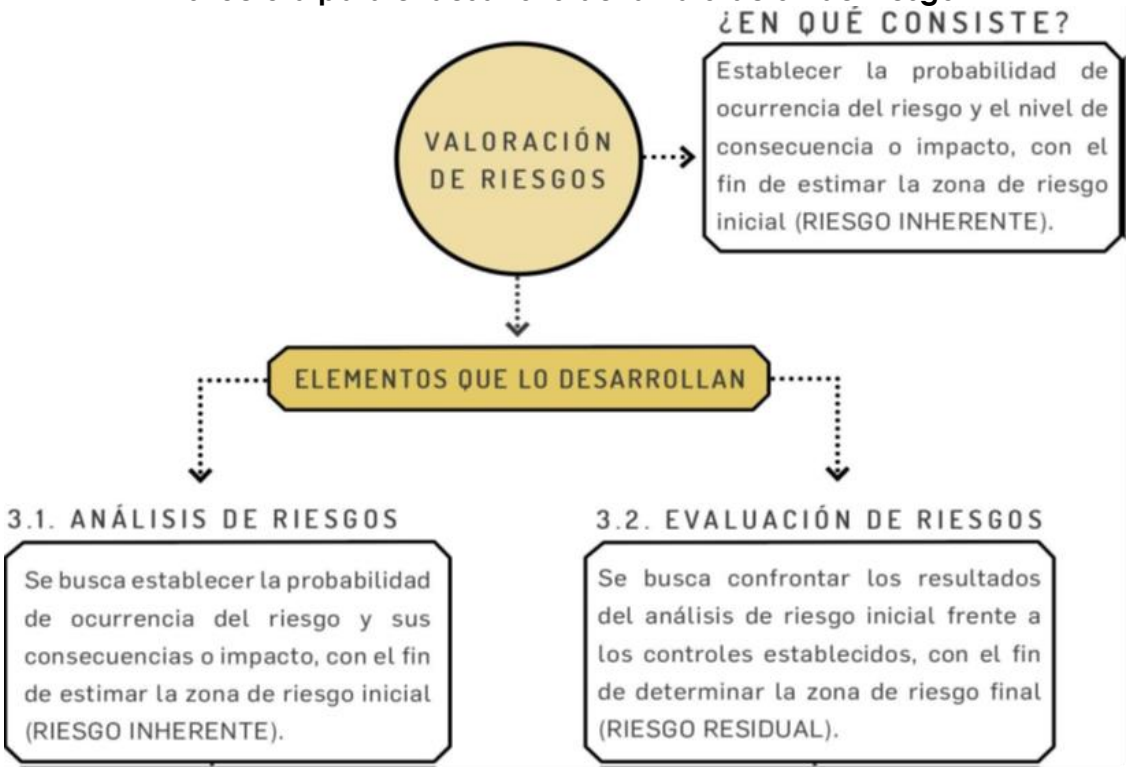
Tabla 3
Clasificación del Riesgo

CLASE	DESCRIPCIÓN
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 Entidad (no participa personal de la Entidad).
Fraude Interno	Pérdida debido a actos de fraude, actuaciones irregulares, comisión de hechos delictivos abuso de confianza, apropiación indebida, incumplimiento de regulaciones legales o internas de la Entidad en las cuales está involucrado por lo menos uno (1) participante interno de la Entidad, 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	Pédida por daños o extravíos de los activos fijos por desastres naturales u otros riesgos/eventos extremos como atentados, vandalismo, orden público.

Fuente: Guía para la administración del riesgo y el diseño de controles en Entidades públicas Versión 5 - diciembre de 2020.

12. VALORACIÓN DEL RIESGO. El Paso de valoración del riesgo incluye dos etapas que la desarrollan: El Análisis y la Evaluación de los riesgos, que se describen a continuación:

Gráfico 6
Estructura para el desarrollo de la valoración del riesgo



Fuente: Guía para la administración del riesgo y el diseño de controles en Entidades Públicas Versión 5 - diciembre de 2020.

12.1. ÁNALISIS DE RIESGOS. Esta etapa busca establecer tanto la probabilidad de ocurrencia del riesgo como su impacto, con el propósito de estimar la zona de riesgo inicial o riesgo inherente.

12.2. DETERMINAR LA PROBABILIDAD. La probabilidad es la posibilidad de ocurrencia del riesgo, la cual está asociada a la exposición al riesgo del proceso.

Para efectos del análisis, la probabilidad de ocurrencia está asociada a la exposición al riesgo del proceso o actividad que se está analizando. De este modo la probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el período de un (1) año, teniendo en cuenta la frecuencia con la que se ejecuta la actividad que genera el riesgo.

12.3. DETERMINAR EL 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.

Los niveles que se deben considerar para calificar la probabilidad e impacto se presentan a continuación:

Gráfico 7
Criterios para definir el nivel de probabilidad e impacto

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

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

Fuente: Guía para la administración del riesgo y el diseño de controles en Entidades Públicas Versión 5 - diciembre de 2020.

La guía permite que el responsable del proceso defina (de acuerdo con su experiencia y conocimiento de las actividades ejecutadas por el proceso) el número de veces que se desarrolla la actividad, cadena de valor del proceso, factores generadores, para identificar el nivel de probabilidad e igualmente para lo que corresponde al impacto.

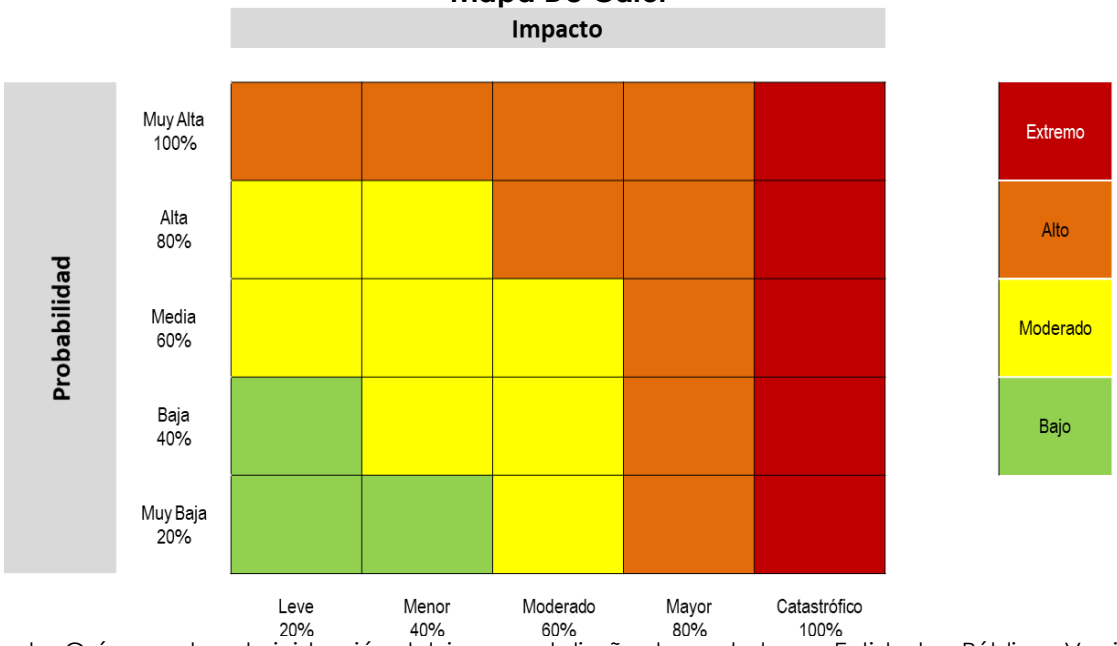
13. EVALUACIÓN DE RIESGOS

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).

13.1. ANÁLISIS PRELIMINAR –RIESGO INHERENTE.

Una vez se tienen claros los factores de probabilidad e impacto se determina el grado de exposición de la Entidad identificando la zona de riesgo bajo, moderado, alto o extremo en la que se califica el riesgo. Este primer análisis, es llamado "Riesgo Inherente" y se define como aquél al que se enfrenta una Entidad en ausencia de acciones por parte de la Dirección para modificar su probabilidad o impacto (Price Water House Cooper, 2005). Se trata de determinar los niveles de severidad a través de la combinación entre la probabilidad y el impacto. Se definen 4 zonas de severidad en la matriz de calor.

Gráfico 8
Mapa De Calor



Fuente: Guía para la administración del riesgo y el diseño de controles en Entidades Públicas Versión 5 - diciembre de 2020.

14. VALORACIÓN DE LOS CONTROLES. En primer lugar, conceptualmente un Control se define como la medida que permite reducir o mitigar el riesgo. Para la Valoración de Controles se debe tener en cuenta:

La identificación de controles se debe realizar a cada riesgo a través de las entrevistas con los responsables de procesos y/o servidores expertos en su quehacer.

Los responsables de implementar y monitorear los controles son los responsables de proceso con el apoyo de su equipo de trabajo.

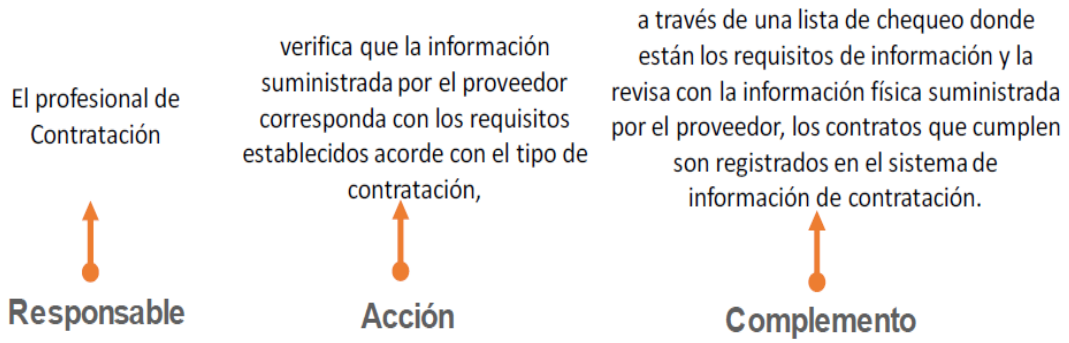
14.1. ESTRUCTURA PARA LA DESCRIPCIÓN DEL CONTROL. Para una adecuada redacción del control se propone una estructura que facilitará más adelante entender su tipología y otros atributos para su valoración. La estructura es la siguiente:

Responsable de Ejecutar el Control: Identifica 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 determina 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.

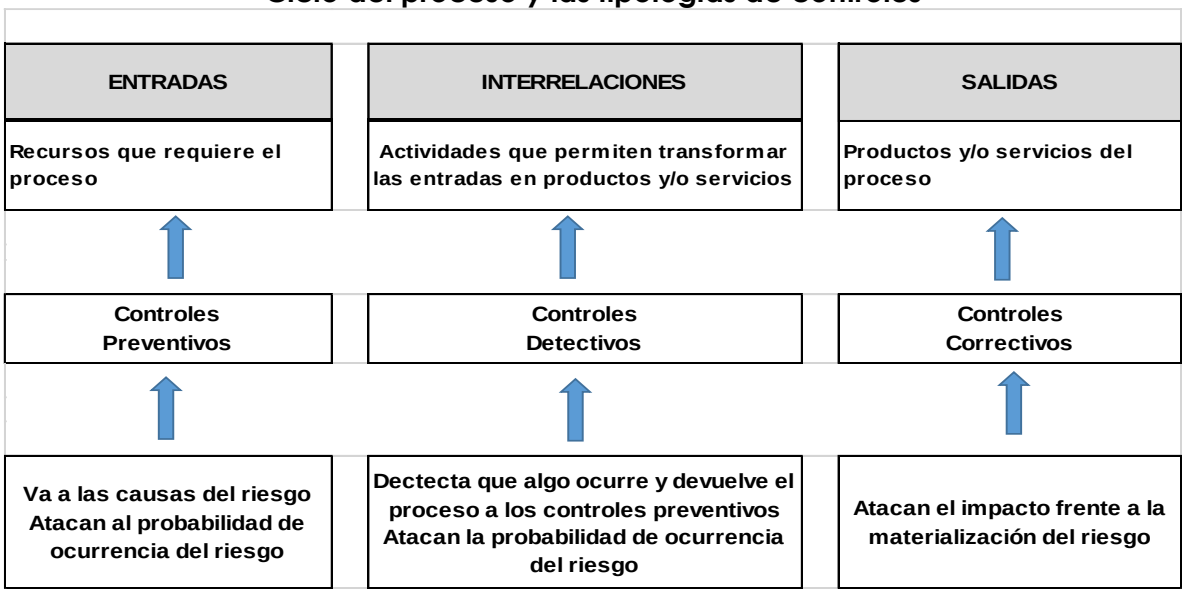
Gráfico 9
Ejemplo de Estructura de Redacción.



Fuente: Guía para la administración del riesgo y el diseño de controles en Entidades públicas Versión 5 - diciembre de 2020. Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

14.2. TIPOLOGÍA DE CONTROLES Y PROCESOS. A través del ciclo de los procesos es posible establecer cuándo se activa un control y, por lo tanto, establecer su tipología con mayor precisión. Para comprender esta estructura conceptual, en la figura siguiente se consideran 3 fases globales del ciclo de un proceso así:

Gráfico 10
Ciclo del proceso y las tipologías de controles



Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

Acorde con lo anterior, tenemos las siguientes 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.

Control Detectivo: Control accionado durante la ejecución del proceso estos controles detectan el riesgo, pero generan reprocesos.

Control Correctivo: Control accionado en la salida del proceso y después de que se materializa el riesgo. Estos controles tienen costos implícitos.

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.

14.3. ANÁLISIS Y EVALUACIÓN DE LOS CONTROLES – Atributos. A continuación, se analizan los atributos para el diseño del control, teniendo en cuenta características relacionadas con la eficiencia y la formalización, se puede observar la descripción y peso asociados a cada tipo de control:

Tabla 4
Atributos de para el diseño del control

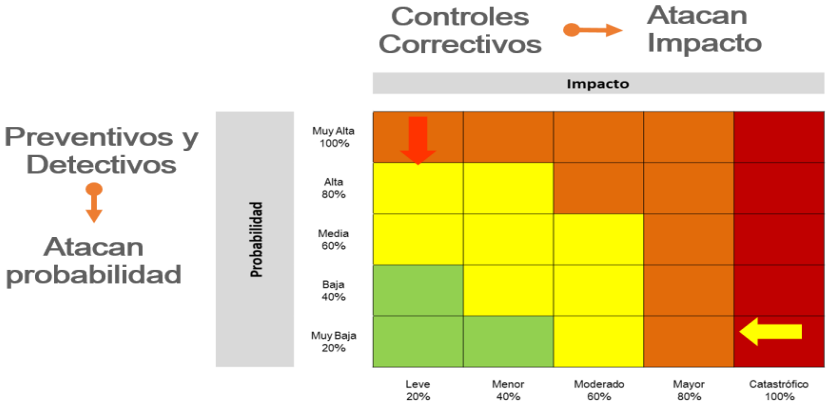
CARACTERISTICAS			DESCRIPCIÓN	PESO
Atributos de Eficiencia	Tipo	Preventivo	Va hacia las causas del riesgo, aseguran el resultado final esperado.	25%
		Dectectivo	Dectecta que algo ocurre y devuelve el proceso a los controles preventivos. Se pueden generar reprocesos.	15%
		Correctivo	Dado que permite reducir el impacto de la materialización del riesgo, tiene 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 ejecutado por una persona, tiene implícito el error humano.	15%
Atributos Informativos	Documentación	Documentado	Controles que estan 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 al 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: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

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

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

Gráfico 11
Movimiento en la matriz de calor acorde con el tipo de control

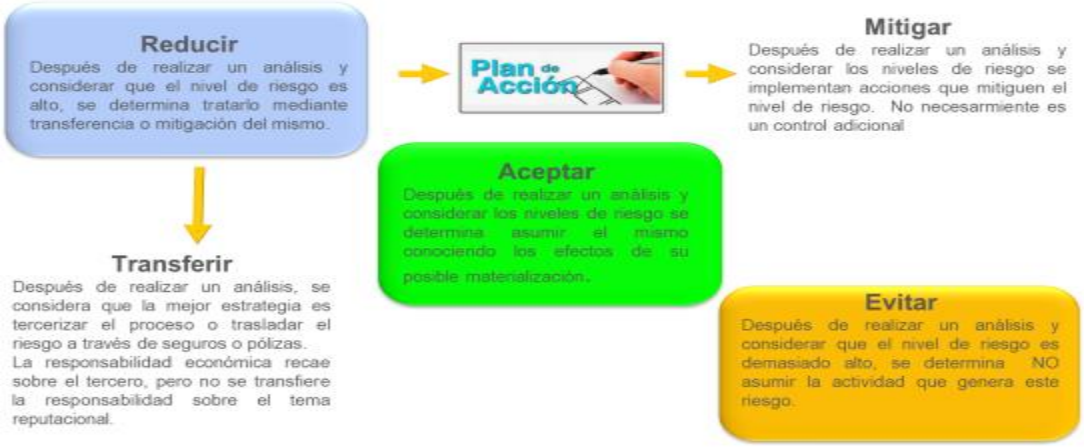


Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

15. 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.

En gráfico 12 se observan las tres opciones mencionadas y su relación con la necesidad de definir planes de acción dentro del respectivo mapa de riesgo.

Gráfico 12



Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

Frente al plan de acción referido para la opción de reducir, es importante mencionar que, conceptualmente y de manera general, se trata de una herramienta de planificación empleada para la gestión y control de planes, programas, actividades y tareas.

Para efectos del mapa de riesgos, cuando se define la opción de reducir, se requerirá la definición de un plan de acción que especifique: a) Responsable, b) Fecha de implementación, y c) Fecha de seguimiento.

15.1. HERRAMIENTAS PARA LA GESTIÓN DEL RIESGO. Como producto de la aplicación de la metodología se contará con los mapas de riesgo. Además de esta herramienta, se tienen las siguientes:

Gestión de Eventos. Un evento es un riesgo materializado, se pueden considerar incidentes que generan o podrían generar pérdidas a la entidad, se debe contar con una base histórica de eventos que permita revisar si el riesgo fue identificado y qué sucedió con los controles. En caso de que el riesgo no se hubiese identificado, se debe incluir y dar el tratamiento correspondiente de acuerdo con la metodología.

Algunas fuentes para establecer una base histórica de eventos pueden ser:

Las PQRD (peticiones, quejas, reclamos, denuncias)

Oficina Jurídica

Líneas Internas de Denuncia

Este mecanismo genera información para que el evento no se vuelva a presentar, así mismo, es posible establecer el desempeño de los controles así:

Desempeño del Control= # eventos / frecuencia del riesgo (# veces que se hace la actividad).

Indicadores Clave de Riesgo. Hace referencia a una colección de datos históricos, por periodos de tiempo, relacionados con algún evento cuyo comportamiento puede indicar una mayor o menor exposición a determinados riesgos. No indica la materialización de los riesgos, pero sugiere que algo no funciona adecuadamente y, por lo tanto, se debe investigar.

15.2. GESTION DE LOS RIESGOS DE POSIBLES HECHOS DE CORRUPCIÓN

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

"Esto implica que las prácticas corruptas son realizadas por actores públicos y/o privados con poder e incidencia en la toma de decisiones y la administración de los bienes públicos" (Conpes N° 167 de 2013).

Para identificar un riesgo de corrupción es necesario que en la descripción del riesgo concurran los componentes de su definición, así:

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

Este tipo de riesgo se establece sobre los procesos y deben estar redactado de manera clara y precisa para evitar ambigüedades o confusiones con la causa generadora identificada.

Así mismo, el proceso de identificación o revisión se debe llevar a cabo anualmente, por los responsables de los procesos, no obstante, están sujetos a ajustes y modificaciones después de su publicación y durante el respectivo año de vigencia, siempre y cuando esté orientado a mejorar el mapa de riesgos y se asegure el histórico de cambios y trazabilidad.

El monitoreo y evaluación lo ejecutan los responsables del proceso con su equipo de trabajo, en concordancia con la cultura del autocontrol y apropiación por parte de todo el Talento Humano de ESE HLCI.

El Jefe de la Oficina de Control Interno, o quien haga sus veces, debe adelantar seguimiento a la gestión de riesgos de corrupción. Los procesos de auditoría interna deben incluir el análisis de las causas, los riesgos de corrupción y la efectividad de los controles incorporados en el mapa de riesgos de corrupción.

15,3. GESTION DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

En primer lugar, se debe tener en cuenta que la política de seguridad digital se vincula al modelo de seguridad y privacidad de la información (MSPI) 3, el cual se encuentra alineado con el marco de referencia de arquitectura TI y soporta transversalmente los otros habilitadores de la política de gobierno digital: seguridad de la información, arquitectura, servicios ciudadanos digitales.

15.3.1. Identificación de los Activos de Seguridad de la Información. Un activo, es cualquier elemento que tenga valor para la Entidad, sin embargo, en el contexto de Seguridad Digital, son activos elementos tales como: Aplicaciones de la Entidad, Servicios web, Redes, Información Física o Digital, Tecnologías de Información -TI, Tecnologías de Operación -TO que utiliza la Entidad para funcionar en el entorno digital. Así la Entidad puede saber qué es lo que debe proteger para garantizar tanto su funcionamiento interno como su funcionamiento de cara al ciudadano, aumentando así su confianza en el uso del entorno digital.

15.3.2. Identificación del Riesgo de Seguridad de la Información. En la identificación de las amenazas es necesario tener en cuenta cuáles y cuantos activos de información tiene cada proceso bajo su responsabilidad. Es importante considerar que las amenazas pueden causar daño temporal o permanente a los activos, procesos y sistemas de soporte de la Entidad. Algunas amenazas pueden afectar

a más de un activo y pueden causar diferentes impactos dependiendo de los activos que se vean afectados.

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.

De acuerdo con lo definido en la "Guía para la administración del riesgo y el diseño de controles en Entidades públicas" versión 05, 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.

Las Vulnerabilidades, son fallas o debilidades que afectan la confidencialidad, integridad y disponibilidad de los sistemas. La identificación podrá obtenerse de pruebas de vulnerabilidad, visitas, entrevistas y/o basados en los criterios que la Entidad vea necesario

Tabla 5
Amenazas y vulnerabilidades de acuerdo con el tipo de activo

TIPO DE ACTIVO	EJEMPLO DE VULNERABILIDADES	EJEMPLO DE AMENAZAS
HARDWARE	Mantenimiento insuficiente	Incumplimiento en el mantenimiento sistema de información.
	Ausencia de esquemas de remplazo periódicos.	Destrucción de equipos o medios
	Ausencia de un eficiente control de cambio en la configuración.	Error en el uso
	Susceptibilidad a las variaciones de temperatura	Pérdida del sumistro de energía
	Almacenamiento de medios sin protección	Hurto de medios o documentos
SOFTWARE	Ausencia de parches de auditoría	Abuso de derechos
	Ausencia de Documentación	Error en el uso
	Tablas de contraseñas sin protección	Falsificación de derchos
	Ausencia de control de cambios eficaz	Manipulación con softw are
RED	Arquitectura de red insegura	Espionaje remoto
	Envío de contraseñas en el texto claro	Espionaje remoto
	Gestión inadecuada de la red	Saturación del sistema de información
PERSONAL	Ausencia de personal	Incumplimiento en la disponibilidad del personal
	Falta de conciencia acerca de la seguridad	Error en el uso
	Ausencia de políticas para el uso correcto del correo electrónico.	Uso no autorizado del equipo.
ENTIDAD	Ausencia de auditorías	Abuso de derechos
	Ausencia de procedimiento formal para el registro y retiro de usuarios.	Abuso de derechos
	Ausencia de procedimientos de control de cambios.	Incumplimiento en el mantenimiento del sistema de información.
	Ausencia de peocedimientos para el manejo de la información.	Error en el uso

Fuente: Ministerio de Tecnologías de la Información y Comunicaciones Min TIC, 2018.

15.4. GESTION DE LOS RIESGOS DEL SISTEMA DE SEGURIDAD Y SALUD EN EL TRABAJO

La identificación y gestión de los Riesgos del Sistema de Seguridad y Salud en el Trabajo, se realiza mediante la aplicación del procedimiento de "Identificación de peligros, valoración de riesgos y determinación de controles", a través del cual se identifican los peligros y valorar los riesgos para las operaciones y actividades que generen situaciones adversas que puedan poner en riesgo la salud y seguridad de los servidores públicos, contratistas y visitantes de la ESE Hospital Local Cartagena de Indias.

15.5. GESTIÓN DE LOS RIESGOS EN LOS PROCESOS DE CONTRATACIÓN

Atendiendo los lineamientos establecidos en el "Manual para la Identificación y Cobertura del Riesgo en los Procesos de Contratación", de Colombia Compra Eficiente, y en el Manual de Interventoría y Supervisión de la Entidad (Resolución Interna 001de 20179), los responsables de la elaboración de los estudios previos, junto con el grupo interdisciplinario responsable de la parte técnica, financiera y jurídica del proyecto deberán atender los siguientes pasos:

Establecer el contexto.

Identificar y clasificar los riesgos.

Evaluar y calificar los riesgos.

Asignación y tratamiento de los riesgos.

Monitorear los riesgos.

Para desarrollar cada uno de los pasos enunciados anteriormente se debe tener en cuenta lo establecido en el "Manual para la Identificación y Cobertura del Riesgo en los Procesos de Contratación", publicado en la página web de Colombia Compra Eficiente, en el siguiente enlace de Contratación"https://www.colombiacompra.gov.co/manuales-guias-y-pliegos tipo/manuales-y-guías.

16. ACTUALIZACIÓN DEL MAPA DE RIESGOS

El mapa de riesgos es revisado y actualizado cuando el proceso presente cambios en su objetivo, alcance y/o actividades, o cuando el contexto estratégico presente un cambio significativo que requiera la revisión completa de los riesgos gestionados, teniendo como mínimo una revisión y/o actualización anual a partir de última fecha de revisión.

Los riesgos identificados podrán ser actualizados de forma individual, cuando así se requiera, tomando como insumos las necesidades de ajuste identificadas en auditorías internas, revisión por la dirección, auditorías externas o resultado de las acciones de seguimiento y autocontrol ejecutadas por los líderes y responsables de proceso.

La actualización o ajuste estará a cargo de los líderes y responsables de procesos (primera línea de defensa), quienes con el acompañamiento de la Oficina Asesora de Planeación y basados en las acciones de seguimiento o autocontrol al proceso, las recomendaciones de seguimiento generadas por la Oficina de Control Interno, auditorías internas, revisión por la dirección o auditorías de entes externos de control procederán a realizar los ajustes de los riesgos a su cargo.

15.2. ACCIONES ANTE LOS EVENTOS (Riesgos Materializados)

Tabla 6
Acciones ante materialización de Riesgos

Tipo/Clasificación del Riesgo	Responsable	Acción
Corrupción	Líder de Proceso	1,Informar al Proceso de Direccionamiento Estratégico sobre el hecho encontrado. 2.Una vez surtido el conducto regular establecido por la ESE HLCI, y área y/o dependencia del alcance(normatividad asociada al hecho de corrupción materializado), tramitar la denuncia ante la instancia de control correspondiente. 3.Identificar e implementar las acciones correctivas necesarias y establecer Plan de Mejoramiento para efectuar el análisis de causas y determinar acciones preventivas y de mejora. 4.Definir nuevos controles asociados al riesgo teniendo en cuenta el plan de mejoramiento definido.
	Oficina de Control Interno	1.Informar al líder de proceso, quien analizará la situación y definirá las acciones a que haya lugar. 2.Una vez surtido el conducto regular establecido por la ESE HLCI, y dependiendo del alcance(normatividad asociada al hecho de corrupción materializado), realizar la denuncia ante la instancia de control correspondiente. 3.Informar a la segunda línea de defensa con el fin facilitar el inicio de las acciones correspondientes con el líder del proceso.
Operativos	Líder de Proceso	1.Informar inmeditamente por escrito a la segunda línea de defensa (Oficina Asesora de Planeación), quienes llevaran un consolidado de eventos. 2.Analizar las causas del evento, identificar e implementar las acciones correctivas necesarias y establecer Plan de Mejoramiento para efectuar el análisis de causas y determinar acciones preventivas y de mejora. 3.Verificar los controles y el Plan de Tratamiento del Mapa de Riesgos y tomar las acciones a que haya lugar. En casos de Eventos relacionados con la continuidad del negocio proceder : 4.Aplicar inmediatamente 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. 5.nalizar las causas del evento, identificar e implementar las acciones correctivas necesarias y establecer Plan de Mejoramiento para efectuar el análisis de causas y determinar acciones preventivas y de mejora. 6.Definir nuevos controles asociados al riesgo teniendo en cuenta el plan de mejoramiento definido. 7.Informar al Proceso de Direccionamiento Estratégico sobre el hallazgo y las acciones tomadas.
	Oficina de Control Interno	1.Informar al líder del proceso sobre el hecho encontrado. 2. Informar a la segunda línea de defensa (Oficina Asesora de Planeación) con el fin de facilitar el inicio de las acciones correspondientes con el líder del proceso.
Riesgo no Identificado	Líder de Proceso Oficina Asesora Planeación Oficina de Control Interno Otro.	1.Informar a la segunda línea de defensa (Oficina Asesora de Planeación) con el fin de facilitar el inicio de las acciones correspondientes con el líder del proceso. 2.Incluir el riesgo en el mapa del proceso correspondiente. 3.Proceder a identificar, valorar y realizar seguimiento según metodología.

Proyectó.
René Ibarra Cáceres
Profesional Logístico Administrativo- Control Interno
Trabajador en misión suministrado por Soluciones Efectivas S.A.S

Revisó: Jefe de Oficina de Control Interno.
Revisó: Ejecutivo administrativo- Planeación