POLITICA INSTITUCIONAL PARA LA ADMINISTRACION DEL RIESGO

ESE CARMEN EMILIA OSPINA

Meses:
Abril 2021

Oficina:
Control Interno

Contenido

1. DECLARACION DE LA POLITICA

LA ESE CARMEN EMILIA OSPINA, 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, mediante la asignación de roles y responsabilidades de cada uno de los servidores y contratistas de prestación de servicios de la Entidad (Esquema de las Líneas de Defensa), y la adopción de la metodología propia para el tratamiento, manejo y seguimiento de los riesgos, determinando las acciones de control defectivas, preventivas y correctivas oportunas, con el fin de mantener los niveles de riesgo aceptables.

2. OBJETIVO

Establecer los principios básicos, lineamientos, responsabilidades y directrices que permitan disminuir la probabilidad de ocurrencia y el impacto de todas aquellas situaciones en que se pueda ver expuesta la ESE Carmen Emilia Ospina, mediante la identificación de acciones de control, análisis, valoración y tratamiento de los riesgos de gestión, corrupción y seguridad digital, con el fin de alcanzar de manera eficaz y efectiva la misión y el cumplimiento de los objetivos institucionales.

3. ALCANCE

La presente política aplica para todos y cada uno de los procesos, proyectos y planes institucionales, y los controles serán aplicados por todos los servidores públicos y contratistas de la ESE Carmen Emilia Ospina.

4. DEFINICIONES

Administración de riesgos: 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. El enfoque de riesgos no se determina solamente con el uso de la metodología, sino logrando que la evaluación de los riesgos se convierta en una parte natural del proceso de planeación. (INTOSAI, 2000).

Aceptación de riesgo: Decisión generada por la entidad de aceptar las consecuencias y probabilidad de un riesgo en particular, sin adelantar acciones de reducción y control. La aceptación del riesgo también se deriva del nivel de riesgo o umbral en el cual el Departamento Administrativo de la Defensoría del Espacio Público acepta el riesgo.

Accesibilidad: Acceso universal a la Web, independientemente del tipo de hardware, software, infraestructura de red, idioma, cultura, localización geográfica y capacidades de los usuarios (W3C World Wide Web Consortium). En el contexto colombiano, ha venido asumiéndose como las condiciones que se incorporan en sitios y herramientas web que favorecen el que usuarios en condiciones de deficiencia tecnológica, física o sensorial o en condiciones particulares de entornos difíciles o no apropiados, puedan hacer uso de estos recursos de la Web1.

Activos de información: Se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización.

Amenaza: Causa Potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o una organización.2

Amenaza informática: Una amenaza informática es toda circunstancia, evento o persona que tiene el potencial de causar daño a un sistema en forma de robo, destrucción, divulgación, modificación de datos o negación de servicio.3

Análisis cualitativo: Herramienta subjetiva que estandariza la evaluación de la probabilidad de ocurrencia y el impacto de los riesgos facilitando su evaluación y posibilidad de priorizarlos.

Análisis de riesgo: Uso sistemático de la información para identificar las fuentes y estimar el riesgo NTC-ISO /IEC 27001.

Actitud (apetito) hacia el riesgo: Enfoque de la organización para evaluar y eventualmente buscar, retener, tomar o alejarse del riesgo.

Causa: Medios, circunstancias, situaciones o agentes generadores del riesgo. Algunas fuentes de riesgos son: el recurso humano, los procesos, la tecnología, la infraestructura y los acontecimientos externos.

Comunicación y Consulta: Procesos continuos y reiterativos que una organización lleva a cabo para suministrar, compartir u obtener información e involucrarse en un diálogo con las partes interesadas, con respecto a la gestión del riesgo. .

Consecuencia o impacto: Efectos generados por la ocurrencia de un riesgo que afecta los objetivos o un proceso de la entidad. Pueden ser entre otros, una pérdida, un daño, un perjuicio, un detrimento.

Corrupción: Uso del poder para desviar la gestión de lo público hacia el beneficio privado.

Criterios para la evaluación de riesgos: Términos de referencia o parámetros con base en los cuales se evalúa la importancia de un riesgo. Los criterios para la evaluación del riesgo los establece la organización de acuerdo con sus necesidades y objetivos.

Control: Medida que modifica al riesgo (Procesos, Política, dispositivos, prácticas u otras acciones).

Confidencialidad: Propiedad de la información que determina que esté disponible a personas autorizadas.

Comunicación y consulta: Procesos continuos y reiterativos que una organización lleva a cabo para suministrar, compartir u obtener información e involucrarse en un diálogo con las partes involucradas.

Evento: Presencia o cambio de un conjunto particular de circunstancias. Dependiendo de las consecuencias o impactos que el evento pueda tener, se habla de que se materializa el riesgo para las situaciones en las cuales las consecuencias son negativas y se materializan las oportunidades cuando las consecuencias o impactos son positivos. Identificación del riesgo. Proceso para encontrar, reconocer y describir el riesgo.

Impacto: Consecuencias que puede ocasionar a la organización, la materialización del riesgo.

Mapa de riesgos: Es una herramienta, basada en los distintos sistemas de información, que pretende identificar las actividades o procesos sujetos a riesgo, cuantificar la probabilidad de estos eventos y medir el daño potencial asociado a su ocurrencia.

Nivel de riesgo: Magnitud del riesgo, expresada en términos de la combinación de la probabilidad y las consecuencias o impacto que este tiene.

Plan Anticorrupción y de Atención al Ciudadano: plan que contempla la estrategia de lucha contra la corrupción que debe ser implementada por todas las entidades del orden nacional, departamental y municipal

Política para la gestión del riesgo: Declaración de la dirección y las intenciones generales de una organización con respecto a la gestión del riesgo.

Probabilidad: Oportunidad de que algo suceda. En la terminología de la gestión del riesgo, la palabra "probabilidad (Likelihood)" se utiliza para hacer referencia a la oportunidad de que algo suceda, esté o no definido, medido o determinado objetiva o subjetivamente, cualitativa o cuantitativamente, y descrito utilizando términos generales o matemáticos (como la probabilidad numérica (Probability) o la frecuencia en un periodo de tiempo determinado).

Tolerancia al riesgo: son los niveles aceptables de desviación relativa a la consecución de objetivos. Pueden medirse y a menudo resulta mejor, con las mismas unidades que los objetivos correspondientes. Para el riesgo de corrupción la tolerancia es inaceptable.

Tratamiento del riesgo: Proceso para modificar el riesgo. El tratamiento del riesgo puede implicar: Evitar el riesgo decidiendo no iniciar o continuar la actividad

que lo originó, tomar o incrementar el riesgo con el fin de perseguir una oportunidad, retirar la fuente del riesgo, cambiar la probabilidad, cambiar las consecuencias, compartir el riesgo con una o varias de las partes (incluyendo los contratos y la financiación del riesgo) y retener el riesgo a través de la decisión informada. En ocasiones se hace referencia a los tratamientos del riesgo relacionados con consecuencias negativas como "mitigación del riesgo", "eliminación del riesgo", "prevención del riesgo" y "reducción del riesgo". El tratamiento del riesgo puede crear riesgos nuevos o modificar los existentes.

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

Valoración del riesgo: Proceso global de identificación del riesgo, análisis del riesgo y evaluación del riesgo.

5. REPONSABILIDADES Y ROLES

Basados en las líneas de defensas establecidas en el Modelo Integrado de Planeación y gestión MIPG, se define los responsable y acciones a su cargo, frente a la administración de riesgo en la ESE Carmen Emilia Ospina.

Línea de Defensa	Responsable	Responsabilidades frente al riesgo
Línea Estratégica	Alta Dirección, Comité de Gestión y Desempeño Institucional y comité Institucional de Control Interno	• Revisar, aprobar y socializar la Política de administración del riesgo. • Aprobar el Mapa de Riesgos de Gestión, Corrupción y Riesgos de Seguridad de la Información. • Analizar los riesgos, vulnerabilidades, amenazas que pongan en peligro el cumplimiento de los objetivos estratégicos, planes institucionales, metas, compromisos de la entidad y capacidades para prestar servicios. • Garantizar el cumplimiento de los planes de la entidad. • Realizar seguimiento y análisis periódico a los riesgos institucionales.
Primera Línea	Líderes de Procesos de (Comunicación,	• Identificar, valorar, evaluar y actualizar cuando se requiera, los riesgos que pueden afectar los objetivos, programas, proyectos y planes asociados a su proceso.

	jurídica, talento humano, ambiental, Contratación, TIC, Almacén, Mantenimiento, calidad, financiera, facturación, Disciplinario, Jefes de zonas, Apoyo diagnóstico y terapéutico, Servicios ambulatorios, referencia contrareferencia, SIAU y demás que se estén en esta línea.	• 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. • Desarrollar ejercicios de autoevaluación para establecer la eficiencia, eficacia y efectividad de los controles seleccionados para el tratamiento de los riesgos identificados • Informar a la oficina de planeación (segunda línea) sobre los riesgos materializados en los objetivos, programas, proyectos y planes de los procesos a cargo. • Revisar los planes de acción establecidos en los riesgos materializados, con el fin de que se tomen medidas oportunas y eficaces para evitar la posible repetición del evento • Reportar los avances y evidencias de la gestión de los riesgos dentro de los plazos establecidos (Mapa de Riesgos de Gestión, Corrupción y Seguridad de la Información)
Segunda Línea	Oficina de 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.
	Coordinador del área de Contratación, área financiera, talento humano, TIC, Calidad.	• Monitorear los riesgos identificados y controles definidos por la primera línea de defensa acorde con la estructura de los temas a su cargo o funciones. • Realizar el seguimiento al mapa de riesgos de su proceso. • Orientar a la primera línea de defensa para que identifique, valore, evalúe y gestione los riesgos 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. • 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 • Asesorar de forma coordinada con la Dirección de Planeación, a la primera línea de defensa en la identificación de los riesgos institucionales y diseño de controles. • Llevar a cabo el seguimiento a los riesgos consolidados y presentar dicho informe de seguimiento al CICI según la programación del Plan Anual de Auditoria o reuniones de este comité. • Revisar que se hayan identificado los riesgos significativos que afectan en el cumplimiento de los objetivos de los procesos, incluyendo los riesgos de corrupción. • Hacer seguimiento a que las actividades de control establecidas para la mitigación de los riesgos de los procesos se encuentren documentadas y actualizadas en los procedimientos y los planes de acción establecidos como resultados de las auditorías realizadas, se realicen de manera oportuna, cerrando las causas raíz del problema, evitando en lo posible la repetición de hallazgos o materialización de riesgos

6. ETAPAS PARA LA GESTION DEL RIESGO

6.1. IDENTIFICACION DEL RIESGO

6.1.1. Identificación de los Puntos de riesgo

Son actividades dentro del flujo del proceso donde existe evidencia o se tienen indicios de que pueden ocurrir eventos de riesgo operativo y deben mantenerse bajo control para asegurar que el proceso cumpla con su objetivo

6.1.2. 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.

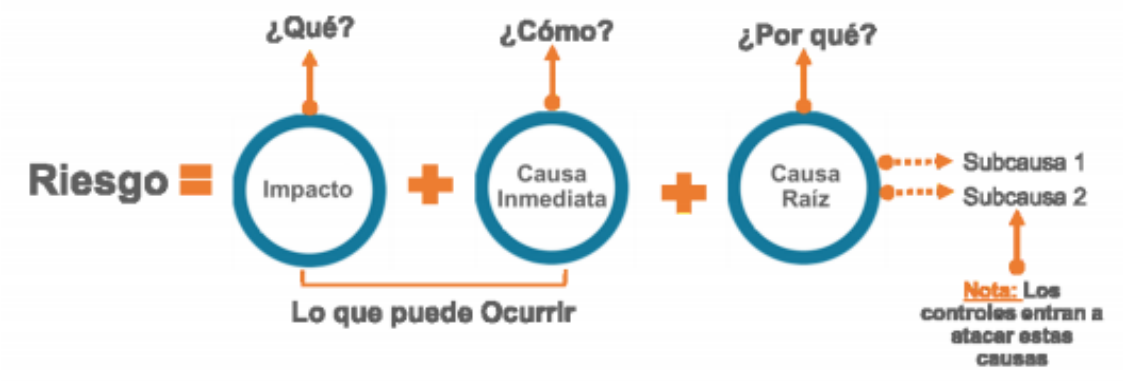
6.1.3. Identificación de áreas de factores de riesgo:

Son las fuentes generadoras de riesgos. En la Tabla 1 encontrará un listado con ejemplo de factores de riesgo que puede tener una entidad.

FACTOR	DEFINICION		DESCRIPCION
Procesos	Eventos relacionados con errores en las actividades que deben realizar los servidores de la organización.		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		Hurto activos
			Posibles comportamientos no éticos de los empleados
			Fraude interno (corrupción, soborno)
Tecnología	Eventos relacionados con la infraestructura tecnológica de la entidad.		Daños de equipos
			Caida de aplicaciones
			Caida 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

6.2. 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 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:



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

Desglosando la estructura propuesta tenemos:

- **Impacto:** las consecuencias que puede ocasionar a la organización 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 puede n existir más de una causa o subcausas que pueden ser analizadas.

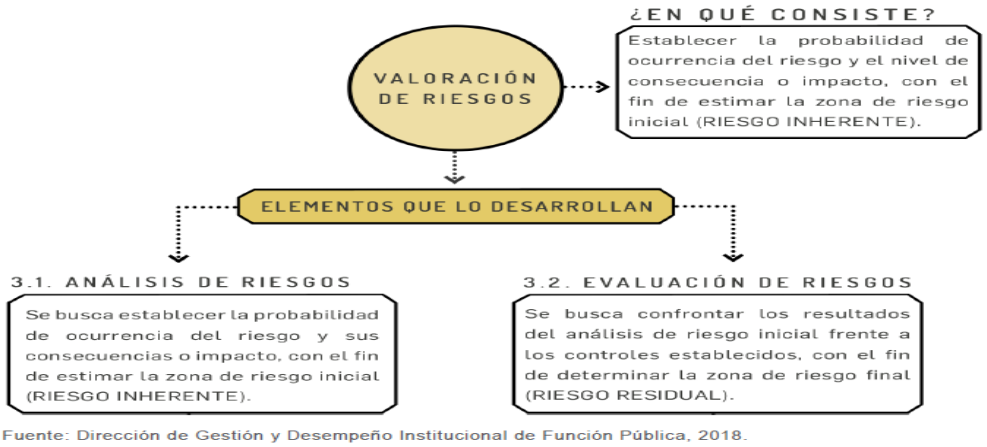
6.3. CLASIFICACION DEL RIESGO

Permite agrupar los riesgos identificados, se clasifica cada uno de los riesgos en las siguientes categorías:

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

6.4. VALORACION DEL RIESGO



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

6.4.1. Determinar la probabilidad

Se entiende como la posibilidad de ocurrencia del riesgo, y estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. De este modo, la probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año.

En las siguientes tablas se presentan los valores de calificación de la probabilidad:

Tabla Criterios para definir el nivel de probabilidad

	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%

6.4.2. 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.

Tabla Criterios para definir el nivel de impacto

	Afectación Económica (o presupuestal)	Pérdida Reputacional
Leve 20%	Afectación menor a 10 SMLMV	El riesgo afecta la imagen de alguna 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 dircetiva y accionistas y/o de provedores
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 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 publicitarios sostenible a nivel país

Frente al análisis de probabilidad e impacto no se utiliza criterio experto, esto quiere decir que el líder del proceso, como conocedor de su quehacer, define cuántas veces desarrolla la actividad, esto para el nivel de probabilidad, y es a través de la tabla establecida que se ubica en el nivel correspondiente, dicha situación se repite para el impacto, ya que no se trata de un análisis subjetivo

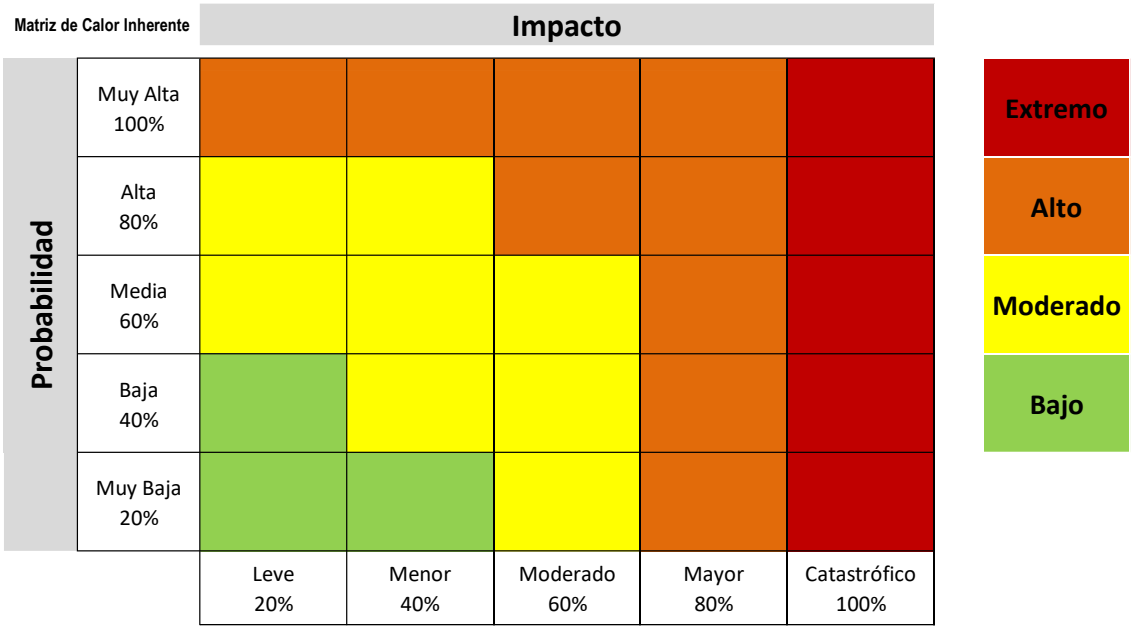
6.5. EVALUACION DEL RIESGO

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).

6.5.1. Riesgo Inherente

Se trata de determinar los niveles de severidad a través de la combinación entre la probabilidad y el impacto

Matriz de calor:



6.5.2. Valoración de 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 líderes de procesos o servidores expertos en su quehacer. En este caso sí aplica el criterio experto.
- Los responsables de implementar y monitorear los controles son los líderes de proceso con el apoyo de su equipo de trabajo.

6.5.3. Tipología 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.

6.5.4. 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

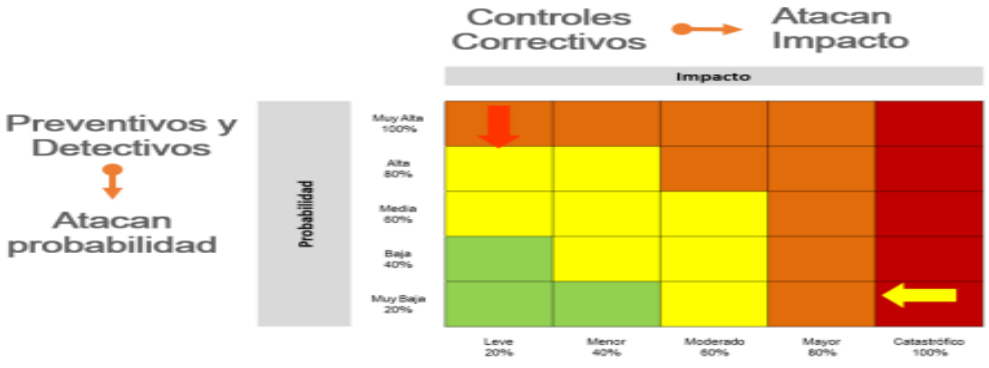
Tabla Atributos de para el diseño del control

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 de Formalización	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	Este atributo identifica a los controles que se ejecutan siempre que se realiza la actividad originadora del riesgo.	-
		Aleatoria	Este atributo identifica a los controles que no siempre se ejecutan cuando se realiza la actividad originadora del riesgo	-
	Evidencia	Con Registro	El control deja un registro que permite evidenciar la ejecución del control	-
		Sin Registro	El control no deja registro de la ejecución del control	-

*Nota 1: Los atributos de formalización se recogerán de manera informativa, con el fin de conocer el entorno del control y complementar el análisis con elementos cualitativos; éstos no tienen una incidencia directa en su efectividad.

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 controles



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

6.5.5. Riesgo residual

Es el resultado de aplicar la efectividad de los controles al riesgo inherente

Para la aplicación de los controles se debe tener en cuenta que los estos mitigan el riesgo de forma acumulativa, esto quiere decir que una vez se aplica el valor de uno de los controles, el siguiente control se aplicará con el valor resultante luego de la aplicación del primer control.

Nota: En caso de no contar con controles correctivos, el impacto residual es el mismo calculado inicialmente, es importante señalar que no será posible su movimiento en la matriz para el impacto

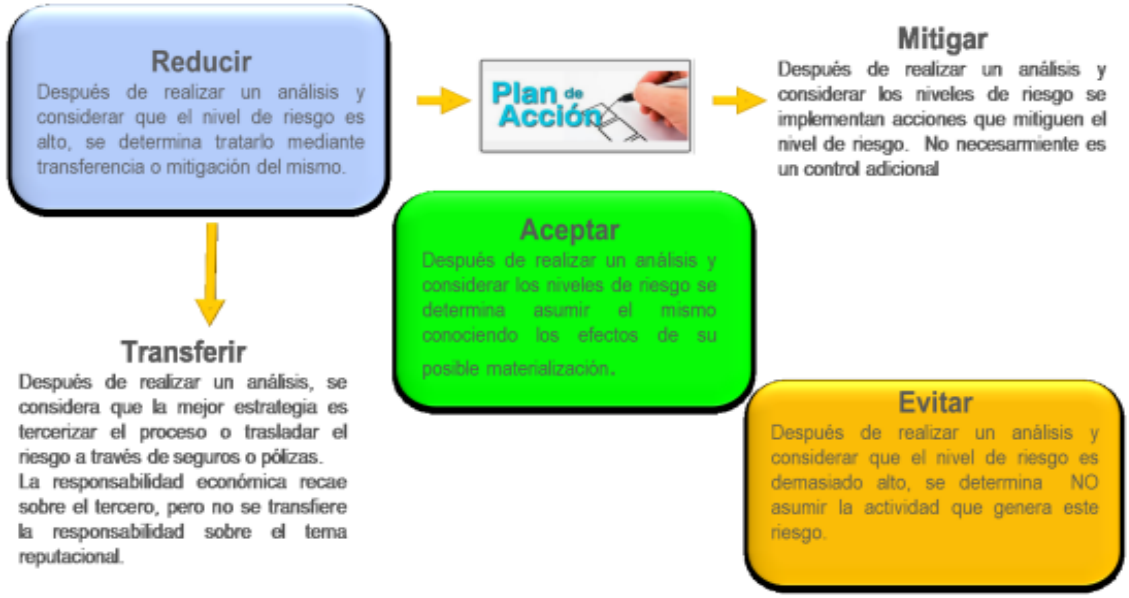
Tabla 8 Aplicación de controles para establecer el riesgo residual

Riesgo	Datos relacionados con la probabilidad e impacto inherentes		Datos valoración de controles		Cálculos requeridos
Posibilidad de pérdida económica por multa y sanción del ente regulador debido a la adquisición de bienes y servicios sin el cumplimiento de los requisitos normativos.	Probabilidad inherente	60%	Valoración control 1 preventivo	40%	60%* 40% = 24% 60% - 24% = **36%**
	Valor probabilidad para aplicar 2° control	36%	Valoración control 2 detectivo	30%	36%* 30% = 10,8% 36% - 10,8% = **25,2%**
	Probabilidad Residual	**25,2 %**			
	Impacto Inherente	80%			
	No se tienen controles para aplicar al impacto	N/A	N/A	N/A	N/A
	Impacto Residual	**80%**			

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

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

6.6.1. Niveles de aceptación del Riesgo

Zona de riesgo **BAJA**: Se ACEPTARÁ el riesgo y se administra por medio de las actividades propias del proyecto o proceso asociado, donde no hay necesidad de plan de mejora

Zona de riesgo **MODERADO**: Se establecerán acciones de control preventivos, detectivos y correctivos según lo pertinente y lo que establezca el líder del proceso, que permitan REDUCIR (transferir o Mitigar) la ocurrencia del riesgo, el cual se plasmara en plan de mejora.

Zona de riesgo **ALTO Y EXTREMO**: Se establecerán acciones de control preventivos, detectivos y correctivos según lo pertinente y lo que establezca el

líder del proceso, que permitan REDUCIR (transferir o Mitigar) o EVITAR la ocurrencia del riesgo, el cual se plasmara en plan de mejora.

Nota: En el caso de riesgos de corrupción, estos no pueden ser aceptados.

7. MONITOREO Y REVISION

Anualmente los líderes de proceso con sus respectivos equipos de trabajo identifican y/o validan los riesgos de gestión, corrupción y seguridad digital asociados al logro de los objetivos de los procesos institucionales.

Para ello, documentarán lo propio y podrán contar con el acompañamiento de la Oficina Asesora de Planeación. Los riesgos de gestión, corrupción y seguridad digital que se encuentren en zona de riesgo BAJO, que soporten documentación de sus controles en procedimientos, se evidencie la implementación de sus controles existentes y no presenten materialización durante la vigencia, pueden ser entrar a ser analizados para no ser objeto de priorización para la vigencia siguiente.

LINES DE DEFENSA	RESPONSABLE	FRECUENCIA	REPORTE
Liena Estrategica	**COMITÉ INSTITUCIONAL DE COORDINACIÓN DE CONTROL INTERNO**	ANUAL	Análisis de los riesgos institucionales
1 linea de Defensa	**LÍDERES DE PROCESO**	**Acorde al nivel de Riesgo Residual**: MODERADO: Bimensual ALTO y EXTREMO: Mensual	Informes de seguimiento sobre los riesgo según el plan de mejora
2 Linea de Defensa	**JEFE OFICINA ASESORA DE PLANEACIÓ**	TRIMESTRAL	* Seguimientos a los mapas de riesgo * Eventos de riesgos que se han materializado en la entidad
3 line a de Defensa	**JEFE OFICINA DE CONTROL INTERNO**	**Riesgo de gestion**: Anual **Riesgo de Corrupcion:** Cuatrimestral	Informes de seguimientos

8. ADMINISTRACION DE RIESGO DE CORRUPCION

En el marco del Plan Anticorrupción y de Atención al Ciudadano establecido en la Ley 1474 de 2011 (artículo 73) y el Decreto 124 de 2016 (artículo 2.1.4.1.) que define las estrategias de lucha contra la corrupción y de atención al ciudadano se definen los lineamientos para la identificación y valoración de riesgos de corrupción que hacen parte del componente 1: gestión del riesgo de corrupción. Es importante recordar que el desarrollo de este componente se articula con los demás establecidos para el desarrollo del plan, ya que se trata de una acción integral en la lucha contra la corrupción.

En materia de riesgos asociados a posibles actos de corrupción, se consideran los siguientes aspectos:

- El riesgo de corrupción se define como la posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.
- Los riesgos de corrupción se establecen sobre procesos.
- El riesgo debe estar descrito de manera clara y precisa. Su redacción no debe dar lugar a ambigüedades o confusiones con la causa generadora de los mismos

8.1. IDENTIFICACIÓN DE RIESGO DE CORRUPCIÓN

A continuación, se señalan algunos de los procesos, procedimientos o actividades susceptibles de actos de corrupción, el cual la ESE Carmen Emilia Ospina podrá adelantar el análisis de contexto interno para la correspondiente identificación de los riesgos.

Direccionamiento estratégico (alta dirección)	● Concentración de autoridad o exceso de poder. Extralimitación de funciones. ● Ausencia de canales de comunicación. ● Amiguismo y clientelismo
Financiero (está relacionado con áreas de planeación y presupuesto)	● Inclusión de gastos no autorizados. ● Inversiones de dineros públicos en entidades de dudosa solidez financiera a cambio de beneficios indebidos para servidores públicos encargados de su administración. ● Inexistencia de registros auxiliares que permitan identificar y controlar los rubros de inversión. ● Inexistencia de archivos contables. ● Afectar rubros que no corresponden con el objeto del gasto en beneficio propio o a cambio de una retribución económica.
De contratación (como proceso o bien los procedimientos ligados a este)	● Estudios previos o de factibilidad deficientes. ● Estudios previos o de factibilidad manipulados por personal interesado en el futuro proceso de contratación. (Estableciendo necesidades inexistentes o aspectos que benefician a una firma en particular). ● Pliegos de condiciones hechos a la medida de una firma en particular. ● Disposiciones establecidas en los pliegos de condiciones que permiten a los participantes direccionar los procesos hacia un grupo en particular. (Ej.: media geométrica). ● Visitas obligatorias establecidas en el pliego de condiciones que restringen la participación. ● Adendas que cambian condiciones generales del proceso para favorecer a grupos determinados. ● Urgencia manifiesta inexistente. ● Concentrar las labores de supervisión en poco personal. ● Contratar con compañías de papel que no cuentan con experiencia.
De información y documentación	● Ausencia o debilidad de medidas y/o políticas de conflictos de interés. ● Concentración de información de determinadas actividades o procesos en una persona. ● Ausencia de sistemas de información que pueden facilitar el acceso a información y su posible manipulación o adulteración. ● Ocultar la información considerada pública para los usuarios. ● Ausencia o debilidad de canales de comunicación
De Investigación y Sanción	● Inexistencia de canales de denuncia interna o externa. ● Dilatar el proceso para lograr el vencimiento de términos o la prescripción de este. ● Desconocimiento de la ley mediante interpretaciones subjetivas de las normas vigentes para evitar o postergar su aplicación. ● Exceder las facultades legales en los fallos.
De trámites y/o servicios internos y externos	● Cobros asociados al trámite. ● Influencia de tramitadores. ● Tráfico de influencias: (amiguismo, persona influyente).

8.2. LINEAMIENTOS PARA LA IDENTIFICACIÓN DEL RIESGO DE CORRUPCIÓN

Las preguntas clave para la identificación del riesgo son:

8.3. VALORACION DEL RIESGO

8.3.1. Determinar la probabilidad

La determinación de la probabilidad (posibilidad de ocurrencia del riesgo) se debe llevar a cabo de acuerdo con lo establecido en la tabla de criterios de Riesgo de Gestión en el aparte **6.4.1.**

	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%

8.3.2. Determinación de Impacto

Para la determinación del impacto frente a posibles materializaciones de riesgos de corrupción se analizarán únicamente los siguientes niveles i) moderado, ii) mayor, y iii) catastrófico, dado que estos riesgos siempre serán significativos, en tal sentido, no aplican los niveles de impacto leve y menor, que sí aplican para las demás tipologías de riesgos. Ahora bien, para establecer estos niveles de impacto se deberán aplicar las siguientes preguntas frente al riesgo identificado

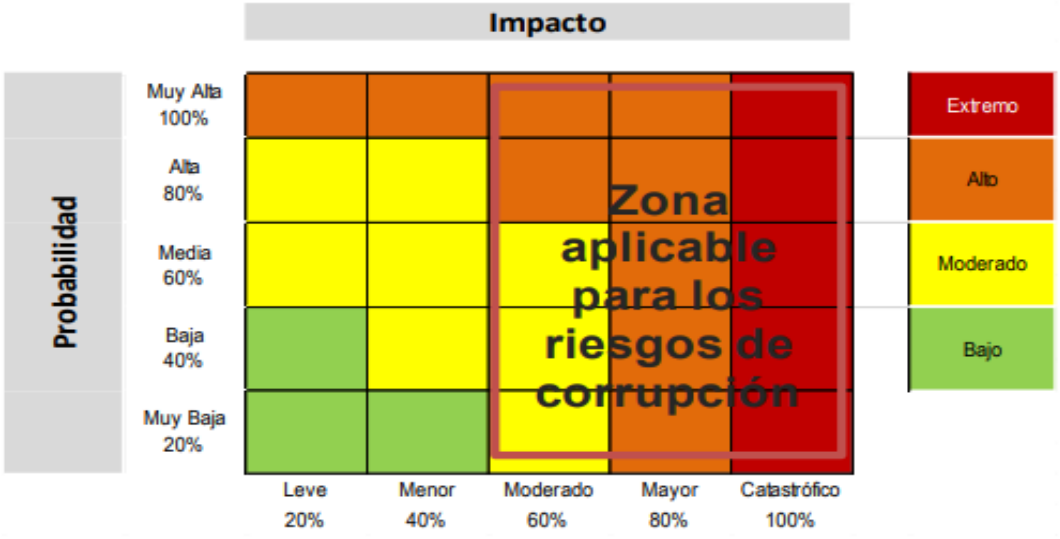
No.	SI EL RIESGO DE CORRUPCIÓN SE MATERIALIZA PODRÍA..	RESPUESTA	
		SI	NO
1	¿Afectar al grupo de funcionarios del proceso?	x	
2	¿Afectar el cumplimiento de metas y objetivos de la dependencia?	x	
3	¿Afectar el cumplimiento de misión de la entidad?	x	
4	¿Afectar el cumplimiento de la misión del sector al que pertenece la entidad?		x
5	¿Generar pérdida de confianza de la entidad, afectando su reputación?	x	
6	¿Generar pérdida de recursos económicos?	x	
7	¿Afectar la generación de los productos o la prestación de servicios?	x	
8	¿Dar lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien, servicios o recursos públicos?		x
9	¿Generar pérdida de información de la entidad?		x
10	¿Generar intervención de los órganos de control, de la Fiscalía u otro ente?	x	
11	¿Dar lugar a procesos sancionatorios?	x	
12	¿Dar lugar a procesos disciplinarios?	x	
13	¿Dar lugar a procesos fiscales?	x	
14	¿Dar lugar a procesos penales?		x
15	¿Generar pérdida de credibilidad del sector?		x
16	¿Ocasionar lesiones físicas o pérdida de vidas humanas?		x
17	¿Afectar la imagen regional?		x
18	¿Afectar la imagen nacional?		x
19	¿Generar daño ambiental?		x
Responder afirmativamente de UNA a CINCO pregunta(s) genera un impacto moderado. Responder afirmativamente de SEIS a ONCE preguntas genera un impacto mayor. Responder afirmativamente de DOCE a DIECINUEVE preguntas genera un impacto catastrófico		**10**	
MODERADO	Genera medianas consecuencias sobre la entidad		
MAYOR	Genera altas consecuencias sobre la entidad		
CATASTRÓFICO	Genera consecuencias desastrosas para la entidad		

Nivel de Impacto Mayor

Por cada riesgo de corrupción identificado, se debe diligenciar una tabla de estas

8.3.3. Análisis preliminar (riesgo inherente)

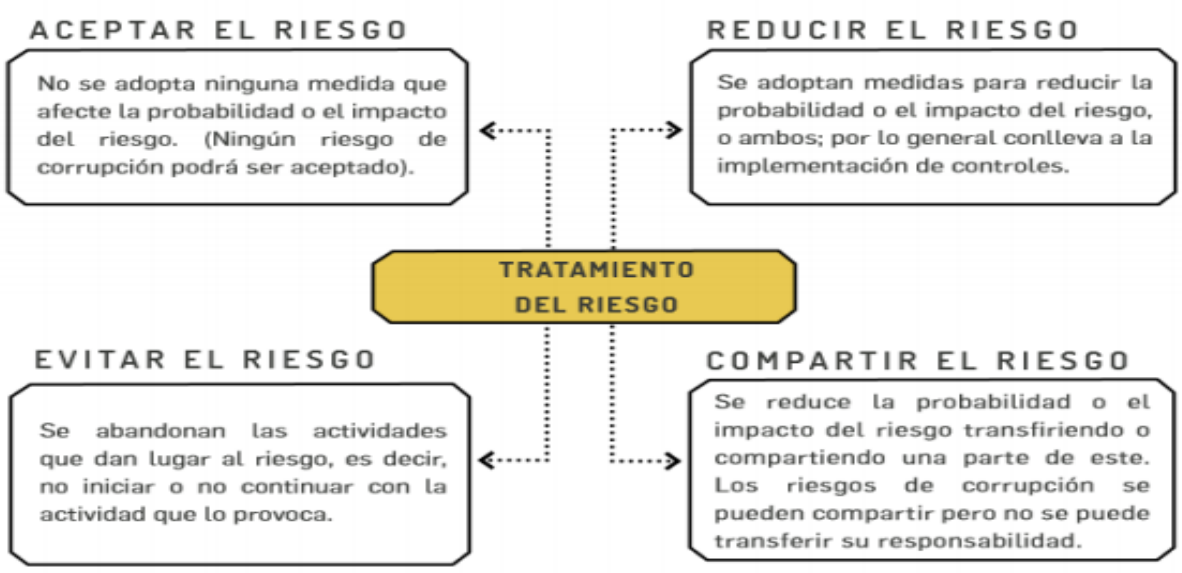
En esta etapa se define el nivel de severidad para el riesgo de corrupción identificado, para lo cual se aplica la matriz de calor establecida en el numeral **6.5.1**., teniendo en cuenta el ajuste frente a los niveles de impacto insignificante y menor mencionados en la determinación del impacto, lo que implica que las zonas de severidad para este tipo de riesgos se delimitan como se muestra a continuación:



Fuente: Elaboración conjunta entre la Dirección de Gestión y Desempeño Institucional de Función Pública la Secretaría de Transparencia, 2018.

8.3.4. Valoración de controles

La valoración de controles son los mismos establecidos para los riesgos de gestión contemplados en el numeral **6.5.2.**



Para los riesgos de corrupción: se establece el siguiente nivel:

Ningún riesgo de corrupción podrá ser aceptado.

Zona de riesgo MODERADA Se establecen acciones de control preventivas que permitan REDUCIR la probabilidad de ocurrencia del riesgo.

Zona de riesgo ALTA y EXTREMA Se adoptan medidas para:

REDUCIR la probabilidad o el impacto del riesgo, o ambos; por lo general conlleva a la implementación de controles.

EVITAR Se abandonan las actividades que dan lugar al riesgo, decidiendo no iniciar o no continuar con la actividad que causa el riesgo.

TRANSFERIR O COMPARTIR una parte del riesgo para reducir la probabilidad o el impacto del mismo.

8.3.5. Monitoreo y Seguimiento de riesgos de corrupción

El gerente de la ESE C.E.O y los líderes de los procesos, en conjunto con sus equipos, deben monitorear y revisar periódicamente la gestión de riesgos de corrupción y si es el caso ajustarlo (primera línea de defensa). Le corresponde, igualmente, a la oficina de planeación adelantar el monitoreo (segunda línea de defensa).

El Jefe de Control Interno o quien haga sus veces, debe adelantar seguimiento al Mapa de Riesgos de Corrupción.

- Primer seguimiento: Con corte al 30 de abril. En esa medida, la publicación deberá surtirse dentro de los diez (10) primeros días del mes de mayo.
- Segundo seguimiento: Con corte al 31 de agosto. La publicación deberá surtirse dentro de los diez (10) primeros días del mes de septiembre.
- Tercer seguimiento: Con corte al 31 de diciembre. La publicación deberá surtirse dentro de los diez (10) primeros días del mes de enero.

El seguimiento adelantado por la Oficina de Control Interno se deberá publicar en la página web de la entidad o en un lugar de fácil acceso para el ciudadano

9. ADMINISTRACION DE 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), 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

9.1. IDENTIFICACIÓN DE LOS ACTIVOS DE SEGURIDAD DE LA INFORMACIÓN

9.1.1. Identificación de los activos de seguridad de la información

Un activo es cualquier elemento que tenga valor para la organización, sin embargo, en el contexto de seguridad digital, son activos elementos tales como:

- Aplicaciones de la organización.
- Servicios web
- Redes

- Información física o digital
- Tecnologías de información TI
- Tecnologías de operación TO que utiliza la organización para funcionar en el entorno digital

La identificación de activos, nos permite determinar qué es lo más importante que cada entidad y sus procesos poseen (sean bases de datos, archivos, servidores web o aplicaciones clave para que la entidad pueda prestar sus servicios) a la vez se 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.

9.1.2. Identificación del riesgo

Se podrán identificar los siguientes tres (3) riesgos inherentes de seguridad de la información:

- Pérdida de la confidencialidad
- Perdida de Integridad
- Perdida 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.

9.1.3. Identificación de Amenazas

Se plantean los siguientes listados de amenazas, que representan situaciones o fuentes que pueden hacer daño a los activos y materializar los riesgos.

- Deliberadas (D) fortuitas (F) ambiental (A).

Tipo	Amenaza	Origen
Daño físico	Fuego	F, D, A
	Agua	F, D, A
	Contaminación	F, D, A
	Accidente Importante	F, D, A
	Destrucción del equipo o medios	F, D, A
	Polvo, corrosión, congelamiento	F, D, A
Eventos naturales	Fenómenos climáticos	A
	Fenómenos sísmicos	A
	Fenómenos volcánicos	A
	Fenómenos meteorológicos	A
	Inundación	A
Perdida de los servicios esenciales	Fallas en el sistema de suministro de agua o aire acondicionado	A
	Perdida de suministro de energía	A
	Falla en equipo de telecomunicaciones	D, F
Perturbación debida a la radiación	Radiación electromagnética	D, F
	Radiación térmica	D, F
	Impulsos electromagnéticos	D, F
	Interceptación de señales de interferencia comprometida	D
	Espionaje remoto	D
	Escucha encubierta	D
	Hurto de medios o documentos	D
	Hurto de equipo	D
	Recuperación de medios reciclados o desechados	D
Compromiso de la información	Divulgación	D, F
	Datos provenientes de fuentes no confiables	D, F
	Manipulación con hardware	D
	Manipulación con software	D
	Detección de la posición	D, F
	Fallas del equipo	F
	Mal funcionamiento del equipo	F
	Saturación del sistema de información	F
Fallas técnicas	Mal funcionamiento del software	F
	Incumplimiento en el mantenimiento del sistema de información.	F
Acciones no autorizadas	Uso no autorizado del equipo	D
	Copia fraudulenta del software	D
	Uso de software falso o copiado	D
	Corrupción de los datos	D
	Procesamiento ilegal de datos	D
Compromiso de las funciones	Error en el uso	D, F
	Abuso de derechos	D
	Falsificación de derechos	D
	Negación de acciones	D
	Incumplimiento en la disponibilidad del personal	D

Amenazas dirigidas por el hombre: empleados con o sin intención, proveedores y piratas informáticos, entre otros.

Fuente de amenaza	*Motivación*	*Acciones amenazantes*
Pirata informático, intruso ilegal	• Reto	• Piratería
	• Ego	• Ingeniería Social
	• Rebelión	• Intrusión, accesos forzados al sistema
	• Dinero	• Acceso no autorizado
Criminal de la computación	• Destrucción de la información	• Crimen por computador
	• Divulgación ilegal de la información	• Acto fraudulento
	• Ganancia monetaria	• Soborno de la información
	• Alteración no autorizada de los datos	• Suplantación de identidad
		• Intrusión en el sistema
Terrorismo	• Chantaje	• Bomba/Terrorismo
	• Destrucción	• Guerra de la información
	• Explotación	• Ataques contra el sistema DDoS
	• Venganza	• Penetración en el sistema
	• Ganancia política	• Manipulación en el sistema
	• Cubrimiento de los medios de comunicación	
Espionaje industrial (inteligencia, empresas, gobiernos extranjeros, otros intereses)	• Ventaja competitiva	• Ventaja de defensa
	• Espionaje económico	• Ventaja política
		• Explotación económica
		• Hurto de información
		• Intrusión en privacidad personal
		• Ingeniería social
		• Penetración en el sistema
		• Acceso no autorizado al sistema
Intrusos (Empleados con entrenamiento deficiente, descontentos, malintencionados, negligentes, deshonestos o despedidos)	• Curiosidad	• Asalto a un empleado
	• Ego	• Chantaje
	• Inteligencia	• Observar información reservada
	• Ganancia monetaria	• Uso inadecuado del computador
	• Venganza	• Fraude y hurto
	• Errores y omisiones no intencionales (ej. Error en el ingreso de datos, error de programación)	• Soborno de información
		• Ingreso de datos falsos o corruptos
		• Interceptación
		• Código malicioso
		• Venta de información personal
		• Errores en el sistema
		• Intrusión al sistema
		• Sabotaje del sistema
		• Acceso no autorizado al sistema.

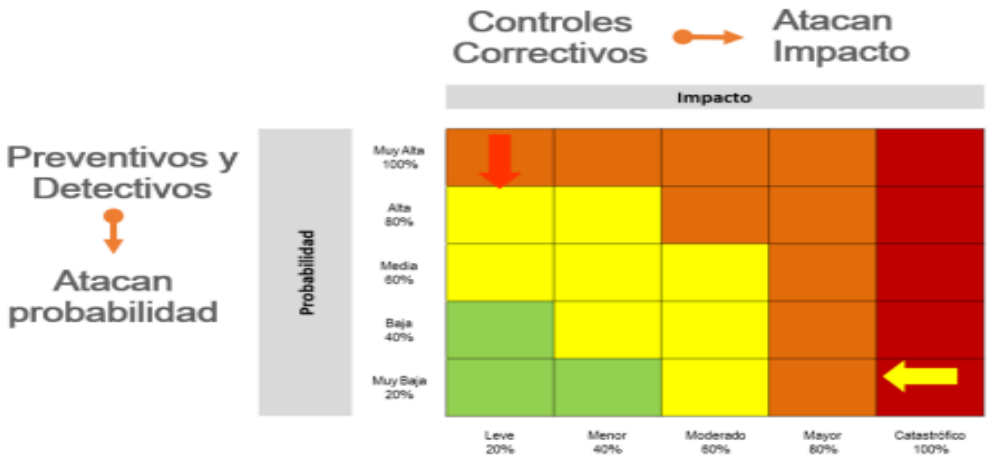
9.1.4. Identificación de vulnerabilidades

La entidad pública puede identificar vulnerabilidades (debilidades) en las siguientes áreas:

Tipo	Vulnerabilidades
Hardware	Mantenimiento insuficiente
	Ausencia de esquemas de reemplazo periódico
	Sensibilidad a la radiación electromagnética
	Susceptibilidad a las variaciones de temperatura (o al polvo y suciedad)
	Almacenamiento sin protección
	Falta de cuidado en la disposición final
	Copia no controlada
Software	Ausencia o insuficiencia de pruebas de software
	Ausencia de terminación de sesión
	Ausencia de registros de auditoría
	Asignación errada de los derechos de acceso
	Interfaz de usuario compleja
	Ausencia de documentación
	Fechas incorrectas
	Ausencia de mecanismos de identificación y autenticación de usuarios
	Contraseñas sin protección
	Software nuevo o inmaduro
Red	Ausencia de pruebas de envío o recepción de mensajes
	Líneas de comunicación sin protección
	Conexión deficiente de cableado
	Tráfico sensible sin protección
	Punto único de falla
Personal	Ausencia del personal
	Entrenamiento insuficiente
	Falta de conciencia en seguridad
	Ausencia de políticas de uso aceptable
	Trabajo no supervisado de personal externo o de limpieza
Lugar	Uso inadecuado de los controles de acceso al edificio
	Áreas susceptibles a inundación
	Red eléctrica inestable
	Ausencia de protección en puertas o ventanas
Organización	Ausencia de procedimiento de registro/retiro de usuarios
	Ausencia de proceso para supervisión de derechos de acceso
	Ausencia de control de los activos que se encuentran fuera de las instalaciones
	Ausencia de acuerdos de nivel de servicio (ANS o SLA)
	Ausencia de mecanismos de monitoreo para brechas en la seguridad
	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)

9.2. VALORACION DE RIESGO

Para esta etapa se asociarán las tablas de probabilidad e impacto definidas en la etapa de Gestión de Riesgo No. 6, manejando la mima matriz de calor.



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

NOTA: La sola presencia de una vulnerabilidad no causa daños por sí misma, ya que representa únicamente una debilidad de un activo o un control, para que la vulnerabilidad pueda causar daño, es necesario que una amenaza pueda explotar esa debilidad. Una vulnerabilidad que no tiene una amenaza puede no requerir la implementación de un control.

9.3. CONTROLES ASOCIADOS A LA SEGURIDAD DE LA INFORMACION

Las entidades públicas podrán mitigar/tratar los riesgos de seguridad digital empleando los siguientes controles, tomados del *Anexo A del estándar ISO/IEC 27001:2013*

Procedimientos operacionales y responsabilidades	Objetivo: asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información
Procedimientos de operación documentados	Control: los procedimientos de operación se deberían documentar y poner a disposición de todos los usuarios que los necesiten.
Gestión de cambios	Control: se deberían controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.
Gestión de capacidad	Control: para asegurar el desempeño requerido del sistema se debería hacer seguimiento al uso de los recursos, llevar a cabo los ajustes y las proyecciones de los requisitos sobre la capacidad futura.
Separación de los ambientes de desarrollo, pruebas y operación	Control: se deberían separar los ambientes de desarrollo, prueba y operación para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.
Protección contra códigos maliciosos	Objetivo: asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.
Controles contra códigos maliciosos	Control: se deberían implementar controles de detección, prevención y recuperación, combinados con la toma de conciencia apropiada por parte de los usuarios para protegerse contra códigos maliciosos.
Copias de respaldo	Objetivo: proteger la información contra la perdida de datos.
Respaldo de información	Control: se deberían hacer copias de respaldo de la información, del *software* y de las imágenes de los sistemas, ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada.

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

ANEXOS

1. Matriz de mapa de riesgo de gestión, corrupción, seguridad de la información.
2. Matriz calificación del impacto riesgo de Corrupción

CONTROL DE CAMBIOS		
Versión	Descripción del cambio	Fecha de aprobación
4	Modificación del documento: Se realiza los siguientes ajustes al documento con en el fin de obtener una mejora continua en el subproceso de planeación 1. Ajustar el documento conforme a las directrices de DAFP en su Guía para la administración del riesgo y el diseño de controles en entidades públicas – versión 5 – diciembre del 2020. 2. Cambio del proceso de control interno a planeación. 3. Cambio tipo de documento y nomenclatura pasa de guía CI-S1-G2 a documento de apoyo GE-S1-D11. 4. Se realiza ajuste estructural y actualización de la vigencia.	15/04/2021
Nombre: Olga Milena Martínez Laguna Contratista Control Interno Nombre: Juan Felipe Cabrera Peña Contratista Área Calidad	Nombre: Eliana Carmenza Ordoñez Argote Contratista Planeación Nombre: Irma Susana Bermúdez Acosta Contratista Área Calidad	Nombre: Jose Antonio Muñoz Paz Cargo: Gerente
Elaboró	**Revisó**	**Aprobó**