telecafé

Expresión de lo nuestro

Política de Operación para la Administración del Riesgo en Telecafé LTDA

www.telecafe.gov.co

@canaltelecafe

telecafé

1.Introducción

TELECAFÉ establece dentro de su gestión estratégica el presente instrumento, el cual es parte esencial para documentar los lineamientos relacionados con los riesgos institucionales (identificación, análisis, valoración, evaluación, tratamiento y respuesta a los riesgos); de tal forma, que se amplíe la capacidad institucional para cumplir adecuadamente la gestión de riesgos ya que es un proceso continuo por tratarse de los riesgos que rodean las actividades desarrolladas dentro de la entidad, pretendiendo de esta manera integrar la gestión de riesgos a la cultura organizacional a través de la política de administración de riesgos dirigida desde la alta dirección, identificando responsables, para que cada servidor público involucre como parte de su qué hacer diario la gestión de riesgos.

Así mismo, se detallan los posibles escenarios de pérdida de continuidad que puedan afectar la misión, el cumplimiento de los objetivos estratégico y la gestión de los procesos, proyectos, programas y planes institucionales, enmarcados en las directrices del Modelo Integrado de Planeación y Gestión -MIPG-, la responsabilidad de las líneas de defensa definidas en el Modelo Estándar de Control Interno -MECI-, los requerimientos de la Guía para la administración del riesgo y el diseño de controles en entidades públicas DAFP, versión 5 de diciembre de 2020 y el Modelo de seguridad y privacidad de la información de la estrategia de Gobierno Digital.

2.Objetivo General

Establecer el marco general de actuación de todos los servidores públicos de la entidad para la adecuada gestión integral de los riesgos y los potenciales escenarios de pérdida de continuidad de negocio, mediante la identificación, análisis, evaluación, tratamiento, monitoreo, revisión, comunicación y consulta de los riesgos que puedan afectar el cumplimiento de la misionalidad y el logro de objetivos institucionales, mejorando las capacidades institucionales de respuesta y orientando la entidad hacia un nivel de aseguramiento razonable.

2.1 Objetivos Específicos

- Comprometer que se desarrollen cada una de las etapas previstas para la actualización e implementación del mapa de riesgos institucional dentro del marco de la Política de Administración del Riesgo de TELECAFÉ LTDA.
- Generar una visión sistémica acerca de la administración y evaluación de riesgos a partir de un ambiente de control y un direccionamiento estratégico adecuados, que fundamenten el desarrollo de las actividades de control.
- Proteger los recursos de la entidad, resguardándolos contra la materialización de los riesgos.

- Introducir dentro de los elementos de control de los procesos de TELECAFÉ LTDA. las acciones de control resultado de la administración del riesgo.
- Involucrar y comprometer a los servidores públicos de la entidad en la búsqueda de acciones y controles encaminados a prevenir y administrar los riesgos con el fin de facilitar y fortalecer el desarrollo de TELECAFÉ LTDA. manteniendo la buena imagen y las buenas prácticas, reconociendo la necesidad de identificar y tratar los riesgos en todos los procesos del canal
- Garantizar la confiabilidad y oportunidad de la información conforme al Direccionamiento Estratégico Institucional.
- Asegurar el cumplimiento de normas, leyes y regulaciones.
- Propiciar el desarrollo efectivo de las actividades misionales en beneficio de la comunidad.

3.Alcance

La Política de Administración de Riesgos es aplicable a todos los procesos de la Entidad y a todas las acciones ejecutadas por los servidores durante el ejercicio de sus funciones en las sedes de Manizales, Pereira y Armenia.

4.Política de Riesgos

TELECAFÉ se compromete a controlar todos aquellos riesgos que pueden impedir el cumplimiento de los objetivos institucionales mediante una efectiva administración de los mismos, como herramienta de gestión que responda a las necesidades de TELECAFÉ, contando con la participación activa de los servidores públicos responsables de los procesos, planes y proyectos quienes deberán identificar, analizar y definir acciones para su prevención.

5.Términos y definiciones

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

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.

Activo de Información: toda aquella información que reside en medio electrónico o físico, que tiene un significado y valor para Colombia Compra Eficiente y, por ende, necesita ser protegida.

Administración del Riesgo: Un 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.

Amenazas: Situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización.

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

Autocontrol: La capacidad que tiene cada servidor público para detectar las desviaciones en su trabajo y realizar los correctivos necesarios; en tal virtud, la autoevaluación, como herramienta complementaria al autocontrol se convierte en un instrumento básico para la mejora continua de las entidades

Autoevaluación: Comprende el monitoreo que se le debe realizar a la operación de la entidad a través de la medición de los resultados generados en cada proceso, procedimiento, proyecto, plan y/o programa, teniendo en cuenta los indicadores de gestión, el manejo de los riesgos, los planes de mejoramiento, entre otros.

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

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

Establecimiento del contexto: Definición de los parámetros internos y externos que se han de tomar en consideración cuando se gestiona el riesgo.

Evento: Ocurrencia o cambio de un particular conjunto de circunstancias. Un evento puede tener una o más consecuencias, o puede tener diferentes causas; puede consistir en algo no ocurrido, y puede ser referido algunas veces como un "incidente" o "accidente".

Eventos potenciales: Hacen referencia a la posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos

Factor de riesgo: Son las fuentes generadoras de riesgos.

Fuentes de riesgo externas: Son eventos asociados a la fuerza de la naturaleza u ocasionados por terceros, que escapan en cuanto a su causa y origen al control de la entidad.

Gestión del Riesgo: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo

Identificación del Riesgo: etapa en la cual se deben establecer las fuentes o factores de riesgo, los eventos o riesgos, sus causas y sus consecuencias.

Impacto: consecuencias o efectos que pueden ocasionar a la organización la materialización del riesgo.

Integridad: Propiedad de exactitud y completitud.

Líder o responsable del proceso: persona con la responsabilidad y autoridad para gestionar un riesgo.

Mapa de Riesgos: Documento que resume los resultados de las actividades de gestión de riesgos, incluye una representación gráfica en modo de mapa de calor de los resultados de la evaluación de riesgos

Matriz de Riesgo: representación final de la probabilidad e impacto de uno o más riesgos frente a un proceso, proyecto o programa.

Marco de referencia para la gestión del riesgo: Conjunto de componentes que brindan las bases y las disposiciones de la organización para diseñar, implementar, monitorear, revisar y mejorar continuamente la gestión del riesgo a través de toda la organización.

MIPG: Modelo Integrado de Planeación y Gestión

MECI: Modelo Estándar de Control Interno

Nivel de riesgo: Es el valor que se determina a partir de combinar la probabilidad de ocurrencia de un evento potencialmente dañino y la magnitud del impacto que este evento traería sobre la capacidad institucional de alcanzar los objetivos. En general la fórmula del Nivel del Riesgo pueder ser Probabilidad * Impacto, sin embargo, pueden relacionarse las variables a través de otras maneras diferentes a la multiplicación, por ejemplo, mediante una matriz de Probabilidad – Impacto. Para el riesgo de corrupción el nivel es inaceptable.

Plan para la Gestión del Riesgo: Esquema dentro del marco de referencia para la gestión del riesgo que especifica el enfoque, los componentes y los recursos de la gestión que se van a aplicar a la gestión del riesgo.

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

Probabilidad: se entiende la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. La probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año.

Propietario del riesgo: Persona o entidad con la responsabilidad de rendir cuentas y la autoridad para gestionar un riesgo.

Proceso para la gestión del riesgo: Aplicación sistemática de las políticas, los procedimientos y las prácticas de gestión a las actividades de comunicación, consulta, establecimiento del contexto, y de identificación, análisis

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: Posibilidad de que suceda algún evento que tendrá un impacto sobre el cumplimiento de los objetivos. Se expresa en términos de probabilidad y consecuencias.

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.

Riesgos de Cumplimiento: Se asocian con la capacidad de la entidad para cumplir con los requisitos legales, contractuales, de ética pública y en general con su compromiso ante la comunidad.

Riesgo Estratégico: Se asocia con la forma en que se administra la Entidad. El manejo del riesgo estratégico se enfoca a asuntos globales relacionados con la misión y el cumplimiento de los objetivos estratégicos, la clara definición de políticas, diseño y conceptualización de la entidad por parte de la alta gerencia.

Riesgos Financieros: Se relacionan con el manejo de los recursos de la entidad que incluyen: la ejecución presupuestal, la elaboración de los estados financieros, los pagos, manejos de excedentes de tesorería y el manejo sobre los bienes. Riesgos de Imagen: están relacionados con la percepción y la confianza por parte de la ciudadanía hacia la institución.

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

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

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

Riesgos de Tecnología: Están relacionados con la capacidad tecnológica de la Entidad para satisfacer sus necesidades actuales y futuras y el cumplimiento de la misión.

Riesgos de Seguridad Digital: Combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas.

Riesgo de Seguridad de la Información: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

SGC: Sistema Gestión de Calidad

TIC: Tecnologías de la Información y las Comunicaciones

Tolerancia al 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.

Valoración del Riesgo: Establecer la probabilidad de ocurrencia del riesgo y el nivel de consecuencia o impacto, con el fin de estimar la zona de riesgo inicial (riesgo inherente). Proceso global de identificación del riesgo, análisis del riesgo y evaluación del riesgo.

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

6.Responsabilidades

Con el fin de realizar análisis y valoración de los riesgos que permitan mitigar efectivamente los riesgos identificados, TELECAFÉ cuenta con los siguientes roles y responsabilidades, definidos mediante las líneas de defensa así:

Líneas de defensa	Responsables	Responsabilidad frente al riesgo
Estratégica	*Alta dirección *Comité de Gerencia *Comité de Gestión y Desempeño Institucional *Comité Institucional de Control Interno	Definir y evaluar la Política de Administración del Riesgo. La evaluación debe considerar su aplicación en la entidad, cambios en el entorno que puedan definir ajustes, dificultades para su desarrollo, riesgos emergentes. Establecer y aprobar la Política de administración del riesgo la cual incluye los niveles de responsabilidad y autoridad.
		Analizar los cambios en el entorno (contexto interno y externo) que puedan tener un impacto significativo en la operación de la entidad y que puedan generar cambios en la estructura de riesgos y controles
		Analizar los riesgos, vulnerabilidades, amenazas y escenarios de pérdida de continuidad de negocio institucionales que pongan en peligro el cumplimiento de los objetivos estratégicos, planes institucionales, metas, compromisos de la entidad y capacidades para prestar servicios.
		Realizar seguimiento y análisis periódico a los riesgos institucionales.
		Realimentar al Comité Institucional de Gestión y Desempeño sobre los ajustes que se deban hacer frente a la gestión del riesgo.

		Evaluar el estado del sistema de control interno y aprobar las modificaciones, actualizaciones y acciones de fortalecimiento del mismo.
		Garantizar el cumplimiento de los planes de la entidad
Primera línea de defensa	Líderes de procesos	Identificar, valorar, evaluar y actualizar cuando se requiera, los riesgos que pueden afectar los objetivos, programas, proyectos y planes asociados a su proceso.
		Definir, adoptar, aplicar y hacer seguimiento a los controles para mitigar los riesgos identificados y proponer mejoras para la gesti ó n del riesgo en sus procesos.
		Supervisar la ejecución de los controles aplicados por el equipo de trabajo en la gestión del día a día, detectar las deficiencias de los controles y determinar las acciones de mejora a que haya lugar.
		Revisar de acuerdo con su competencia y alcance la documentación de continuidad de negocio
		Desarrollar ejercicios de autoevaluación para establecer la eficiencia, eficacia y efectividad de los controles seleccionados para el tratamiento de los riesgos identificados y los planes de preparaci ó n frente a la pérdida de continuidad de negocio.
		Informar a la oficina de planeación (segunda línea) sobre los riesgos materializados en los objetivos, programas, proyectos y planes de los procesos a cargo.
		Reportar en el SIG los avances y evidencias de la gestión de los riesgos dentro de los plazos establecidos.
	Oficina de Planeación	Acompañar, orientar y asesorar a los líderes de procesos en la identificación, análisis, valoración y evaluación del riesgo.
		Supervisar que la primera l í nea identifique, analice, valore, evalúe y realice el tratamiento de los riesgos, que se adopten los controles para la mitigaci ó n de los riesgos identificados y se apliquen las acciones pertinentes para reducir la probabilidad o impacto de los riesgos.

Segunda línea de defensa		Consolidar el Mapa de riesgos institucional (riesgos de mayor criticidad frente al logro de los objetivos) y presentarlo para análisis y seguimiento ante el Comité Institucional de Gestión y Desempeño.
		Monitorear los controles establecidos por la primera línea de defensa acorde con la información suministrada por los líderes de procesos.
		Evaluar que la gestión de los riesgos este acorde con la presente política de la entidad y que sean monitoreados por la primera línea de defensa.
		Promover ejercicios de autoevaluación para establecer la eficiencia, eficacia y efectividad de los controles seleccionados para el tratamiento de los riesgos identificados.
		Orientar y hacer seguimiento a la eficacia de los controles establecidos en los diferentes niveles de operación de la entidad
		Identificar cambios en el apetito del riesgo en la entidad, especialmente en aquellos riesgos ubicados en zona baja y presentarlos para su aprobación del comité institucional de control interno
		Actualizar, según se requiera, los escenarios de riesgo y la documentación asociada al plan de continuidad de negocio bajo su responsabilidad
Tercera línea de defensa	Oficina Asesora de Control Interno	Proporcionar aseguramiento objetivo sobre la eficacia de la gestión del riesgo y control, con énfasis en el diseño e idoneidad de los controles establecidos en los procesos
		Proporcionar aseguramiento objetivo en las áreas identificadas no cubiertas por la segunda línea de defensa
		Asesorar de forma coordinada con la Oficina 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 en los mapas de riesgos de conformidad con el Plan Anual de Auditoria y reportar los resultados al comité institucional de Control Interno
	Recomendar mejoras a la política de administración del riesgo

7.Escenarios de pérdida de continuidad

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

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

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

8.ETAPAS PARA LA GESTIÓN DEL RIESGO

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

Guía para la administración del riesgo y el diseño de controles en entidades públicas - Versión 5 - Diciembre de 2020.pdf

8.1.Determinación de la capacidad del riesgo

Valor máximo que, según el buen criterio de la alta dirección y bajo los requisitos del marco legal aplicable a la entidad, puede ser resistido por la entidad antes de perder total o parcialmente la capacidad de cumplir con sus objetivos; es decir, el valor máximo de la escala resulta de combinar la probabilidad y el impacto.

8.2.Determinación del apetito del riesgo

Luego de determinada la capacidad de riesgo por parte de la alta dirección, estas mismas instancias deben determinar el valor máximo deseable del nivel de riesgo que podría permitir el logro de los objetivos institucionales en condiciones normales de operación del modelo integrado de planeación y gestión en la entidad. Equivale al nivel de riesgo que la entidad puede aceptar, relacionado con sus objetivos, el marco legal y las disposiciones de la alta dirección.

8.3.Determinación de la tolerancia del riesgo

La tolerancia de 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.

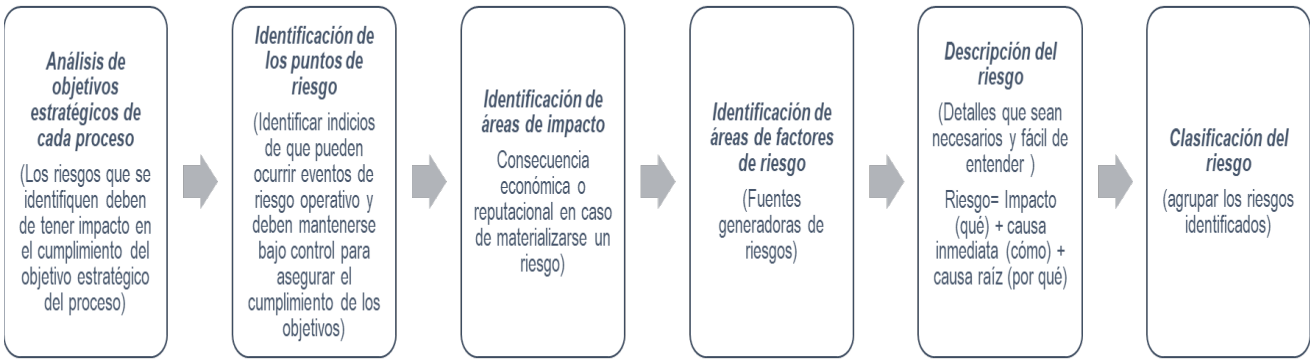
Para determinar la tolerancia de riesgo, se debe definir un valor que es igual o superior al apetito de riesgo y menor o igual a la capacidad de riesgo.

El límite o valor de la tolerancia de riesgo es definido por la alta dirección y aprobada por el órgano de gobierno respectivo y no puede ser superior al valor de la capacidad de riesgo.

La determinación de la tolerancia de riesgo es optativa para la entidad y su uso está limitado a determinar el tipo de acciones para abordar los riesgos, dado que las acciones que se desprendan a partir del análisis de riesgos deben ser proporcionadas y razonables, lo cual se puede determinar en función del valor del nivel de riesgo residual obtenido y su comparación con el apetito y tolerancia de riesgo.

9.IDENTIFICACIÓN DEL RIESGO

Esta etapa tiene como objetivo identificar los riesgos que estén o no bajo el control de la organización, para ello se debe tener en cuenta el contexto estratégico en el que opera la entidad, la caracterización de cada proceso que contempla su objetivo y alcance y, también, el análisis frente a los factores internos y externos que pueden generar riesgos que afecten el cumplimiento de los objetivos.

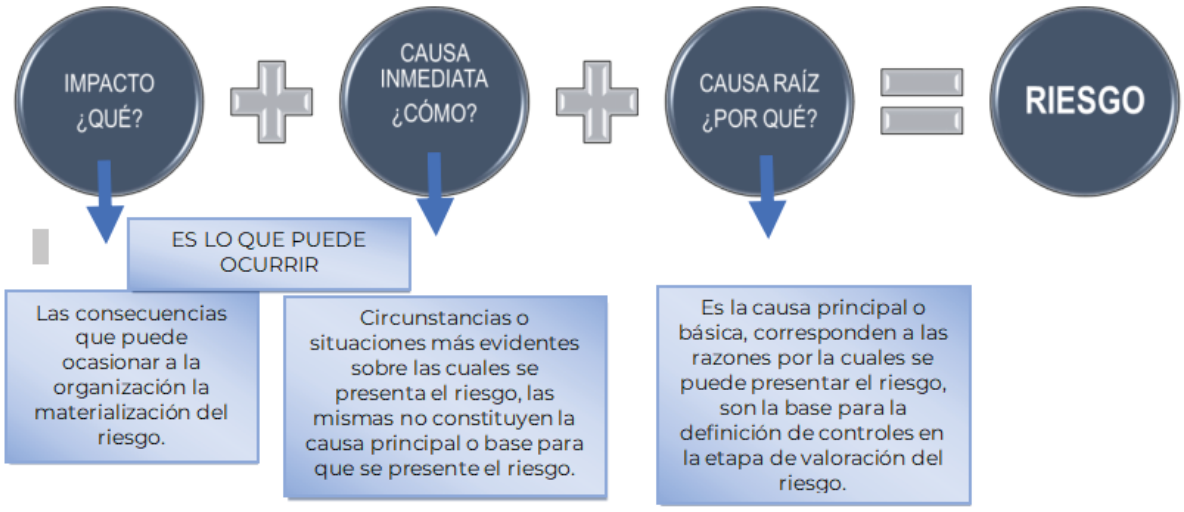


9.1.Factores de Riesgo

Esta etapa tiene como objetivo identificar los riesgos que estén o no bajo el control de la organización, para ello se debe tener en cuenta el contexto estratégico en el que opera la entidad, la caracterización de cada proceso que contempla su objetivo y alcance y, también, el análisis frente a los factores internos y externos que pueden generar riesgos que afecten el cumplimiento de los objetivos.

FACTOR	DEFINICIÓN	DESCRIPCIÓN
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
Talento humano	Incluye seguridad y salud en el trabajo.	Hurto de activos
	Se analiza posible dolo e intención frente a la corrupción	Posibles comportamientos no éticos de los empleados
		Fraude interno (corrupción, soborno)
Producción y Programación	Eventos relacionados con las producciones propias o contratadas y la emisión de programación	Uso inadecuado de equipos
		Hurto de equipos
		Errores humanos
		Emisión de contenidos erróneos
		Caída de pauta
Tecnología	Eventos relacionados con la infraestructura tecnológica de la entidad	Caída de la señal
		Fallas técnicas de emisión
		Daños de equipos
		Daños en la red de transmisión
		Daños en la red de emisión
		Daños en la red de automatización
		Daños en la red de datos
Comercialización y Mercadeo	Eventos relacionados con la comercialización de servicios y productos	Destinación indebida de recursos
		Peculado
		Incumplimiento en los acuerdos
		Inadecuada selección de proveedores
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
		Acceso ilegal a la red de transmisión
		Hackeos de la página web
		Atentados, vandalismo, orden público

9.2 Descripción del riesgo



9.3.Clasificación de riesgos

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

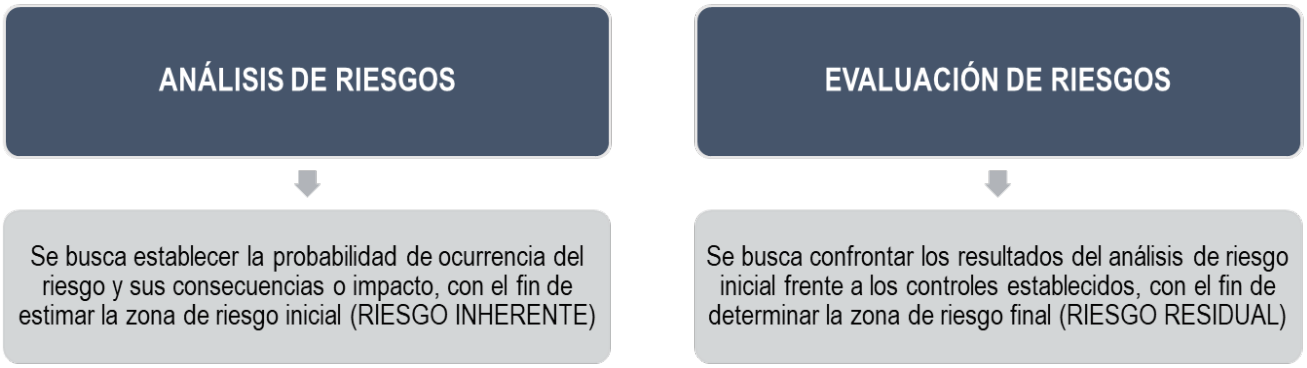
Ejecución y administración de procesos	**Pérdidas derivadas de errores en la ejecución y administración de procesos.**
Fraude externo	Pérdida derivada de actos de fraude por personas ajenas a la organización (no participa personal de la entidad).
Fraude interno	Pérdida debido a actos de fraude, actuaciones 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.
Producción y emisión de contenidos	Errores en la emisión de contenidos
Comercialización y mercadeo	Pérdidas de clientes ocasionados de una mala prestación del servicio o incumplimiento
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.

CLASIFICACIÓN	FACTORES DE RIESGO
Ejecución y administración de procesos	Procesos
Fraude externo	Evento externo
Fraude interno	Talento Humano
Producción y emisión de contenidos	Producción y programación
Comercialización y mercadeo	Comercialización y mercadeo
Fallas tecnológicas	Tecnología
Relaciones laborales	Pueden asociarse a varios factores
Usuarios, productos y prácticas	
Daños a activos fijos/ eventos externos	Infraestructura / Eventos externos

10. Valoración del riesgo

Consiste en establecer la probabilidad de ocurrencia del riesgo y el nivel de consecuencia o impacto, con el fin de estimar la zona de riesgo inicial (RIESGO INHERENTE)

10.1.Análisis y evaluación de riesgos



10.1.1.Determinar la probabilidad

Posibilidad de ocurrencia del riesgo, la cual estará asociada a la exposición del riesgo del proceso o actividad.

Para efectos de este análisis, la probabilidad de ocurrencia 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.

La exposición al riesgo estará asociada al proceso o actividad que se esté analizando, es decir, al número de veces que se pasa por el punto de riesgo en el periodo de 1 año.

	Frecuencia de la Actividad	Probabilidad
Muy baja	La actividad que conlleva el riesgo se ejecuta como máximo 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%

10.1.2.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.

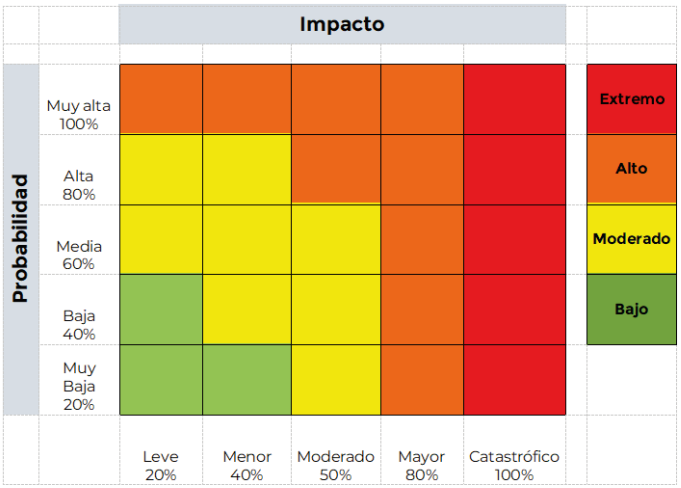
	Afectación económica	Reputacional
Leve 20%	Afectación menor a 10 SMLVM	El riesgo afecta la imagen de algún área de la organización
Menor 40%	Entre 10 y 50 SMLVM	El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, de junta directiva y accionistas y/o proveedores
Moderado 60%	Entre 50 y 100 SMLVM	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 SMLVM	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 SMLVM	El riesgo afecta la imagen a nivel nacional, con efecto publicitario sostenido a nivel país

10.2.Evaluación de riesgos

A partir del análisis de la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto s, se busca determinar la zona de riesgo inicial (RIESGO INHERENTE).

10.2.1.Análisis preliminar (riesgo inherente)

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



Matriz de calor

10.2.2.Valoración de controles

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.

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.

10.2.2.1.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.

10.2.2.2.Tipología de controles

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.

10.2.2.2.1.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.

10.2.2.2.2.Control detectivo

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

10.2.2.2.3.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.

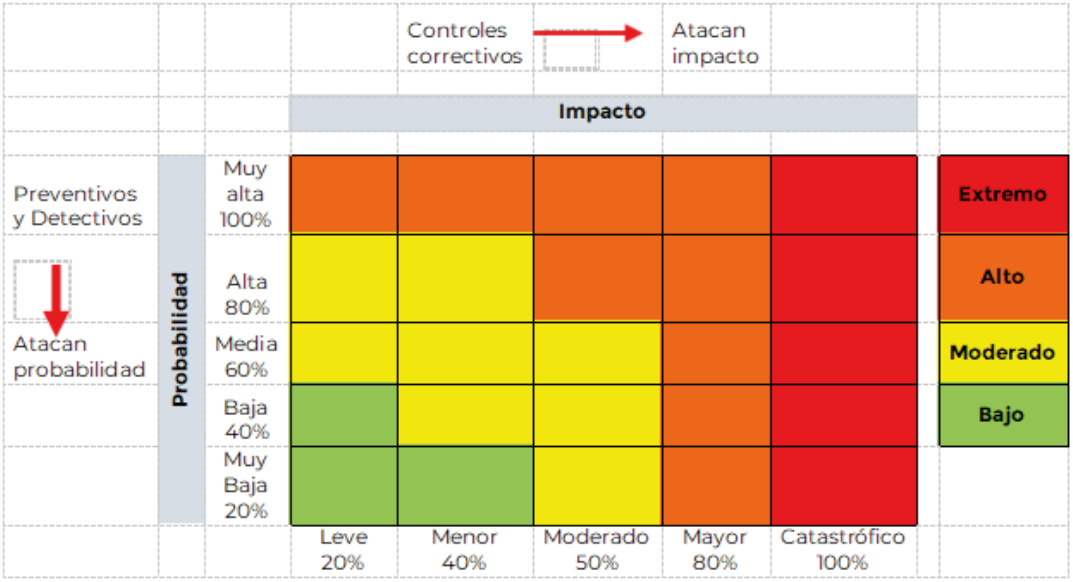
10.2.2.3.Análisis y evaluación de los controles – Atributos

A continuación, se analizan los atributos para el diseño del control, teniendo en cuenta características relacionadas con la eficiencia y la formalización.

	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	10%
Atributos informativos	Documentación	Documentado	Controles que están documentados en el proceso, ya sea en manuales, procedimientos, flujogramas o cualquier otro documento propio del proceso	
		Sin documentar	Identifica a los controles que pese a que se ejecutan en el proceso no se encuentran documentados en ningún documento propio del proceso	
	Frecuencia	Continua	El control se aplica siempre que se realiza la actividad que conlleva el riesgo	
		Aleatoria	El control se aplica aleatoriamente a la actividad que conlleve el riesgo	
	Evidencia	Con registro	El control deja un registro permite evidencia la ejecución del control	
		Sin registro	El control no deja registro de la ejecución del control	

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

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.



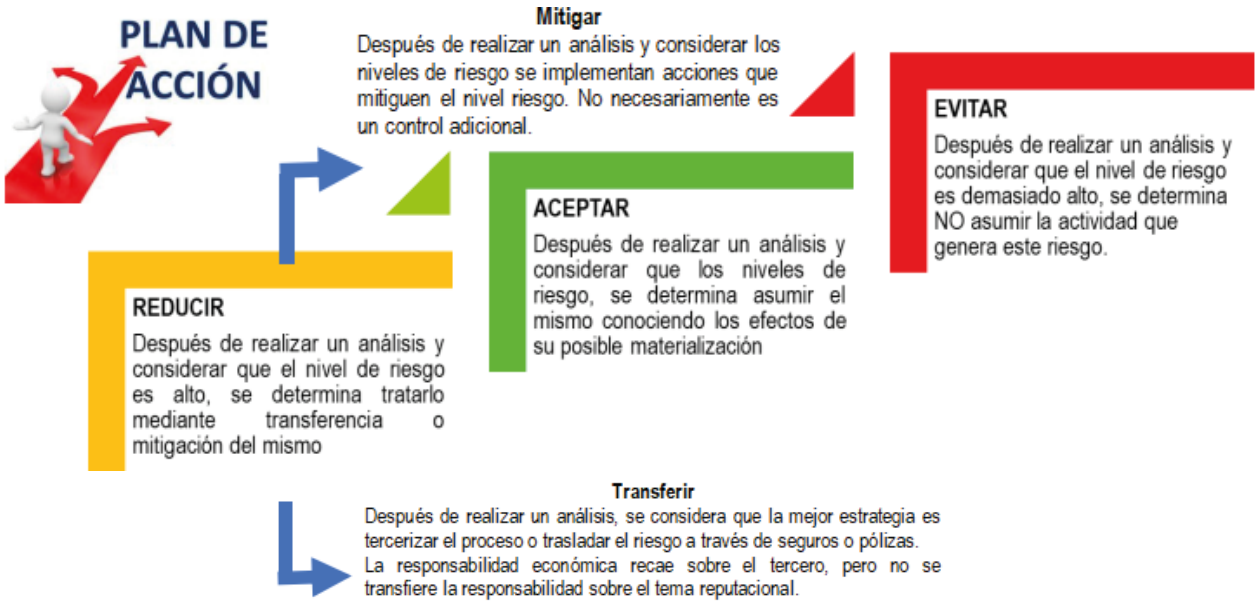
10.2.3.Nivel de riesgo (riesgo residual)

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 controles 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.

10.3.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



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 tareas o proyectos. Para efectos del mapa de riesgos, cuando se define la opción de reducir, se requerirá la definición de un plan de acción que especifique: i) responsable, ii) fecha de implementación, y iii) fecha de seguimiento.

*Nota: El plan de acción es diferente a un plan de contingencia, el cual se enmarca dentro del Plan de Continuidad de Negocio y se consideraría un control correctivo.

telecafé

NIVELES DE ACEPTACIÓN DEL RIESGO

ZONA DE RIESGO RESIDUAL		ESTRATEGIAS DE TRATAMIENTO	APROBACIÓN PLAN DE TRATAMIENTO	JUSTIFICACIÓN Y SEGUIMIENTO
Extremo Alto Moderado	Inaceptable	Evitar Reducir (mitigar y transferir)	Comité Institucional de Coordinación de Control Interno	Debido a que representan mayores niveles de probabilidad e impacto que podrían incidir directamente sobre los objetivos estratégicos, se establecerán controles que permitan reducir el riesgo a niveles aceptables, las cuales serán administradas
Bajo	Aceptable	Evitar Reducir (mitigar y transferir) Aceptar	Líder de Proceso	Considerando que son riesgos que presentan una probabilidad reducida y que de llegarse a materializar no afectarían significativamente el cumplimiento de la estrategia, no obstante, estos serán controlados a través de la definición de puntos de control en el desarrollo de las actividades propias del proceso.

FORMATO MAPA DE RIESGOS

PARTE 1. IDENTIFICACIÓN DEL RIESGO

Proceso	
Objetivo	
Alcance	

Referencia	Causa Inmediata	Causa Raíz	Descripción del Riesgo	Clasificación del Riesgo	Frecuencia	Probabilidad Inherente	%	Impacto Inherente	%	Zona de riesgo inherente

*Nota: La columna referencia se sugiere para mantener el consecutivo de riesgos, así el riesgo salga del mapa no existirá otro riesgo con el mismo número. Una entidad puede ir en el riesgo 150, pero tener 70 riesgos, lo que permite llevar una traza de los riesgos. Esta información la debe administrar la oficina de planeación de la entidad.

No. Control	Descripción del control	Afectación		Tipo		Implementación			Calificación	Atributos		Frecuencia		Evidencia		Probabilidad Residual (2 controles)	Probabilidad residual final	%	Impacto residual final	%	Zona de riesgo final	Tratamiento		
		babili	Impacto	Preventivo	Detectivo	Correctivo	Automático	Manual		Documentado	Sin documentar	Continua	Aleatoria	Con registro	Sin registro							Reducir	Aceptar	Evitar

PARTE 3. PLAN DE ACCIÓN (Para la opción de tratamiento reducir)

Plan de Acción	Responsable	Fecha de Implementación	Fecha de Seguimiento	Seguimiento	Estado

10.4.HERRAMIENTAS PARA LA GESTIÓN DEL RIESGO

Producto de la aplicación de la metodología se contará con los mapas de riesgo.

Además de esta herramienta, se tienen las siguientes:

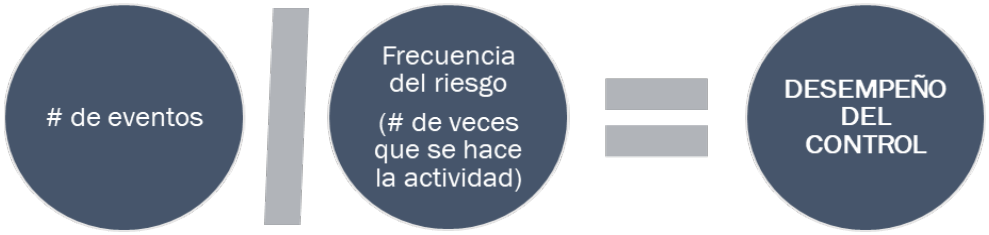
10.4.1.Gestión de eventos

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:

- Mesa de ayuda
- 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:



10.4.1.Gestión de eventos

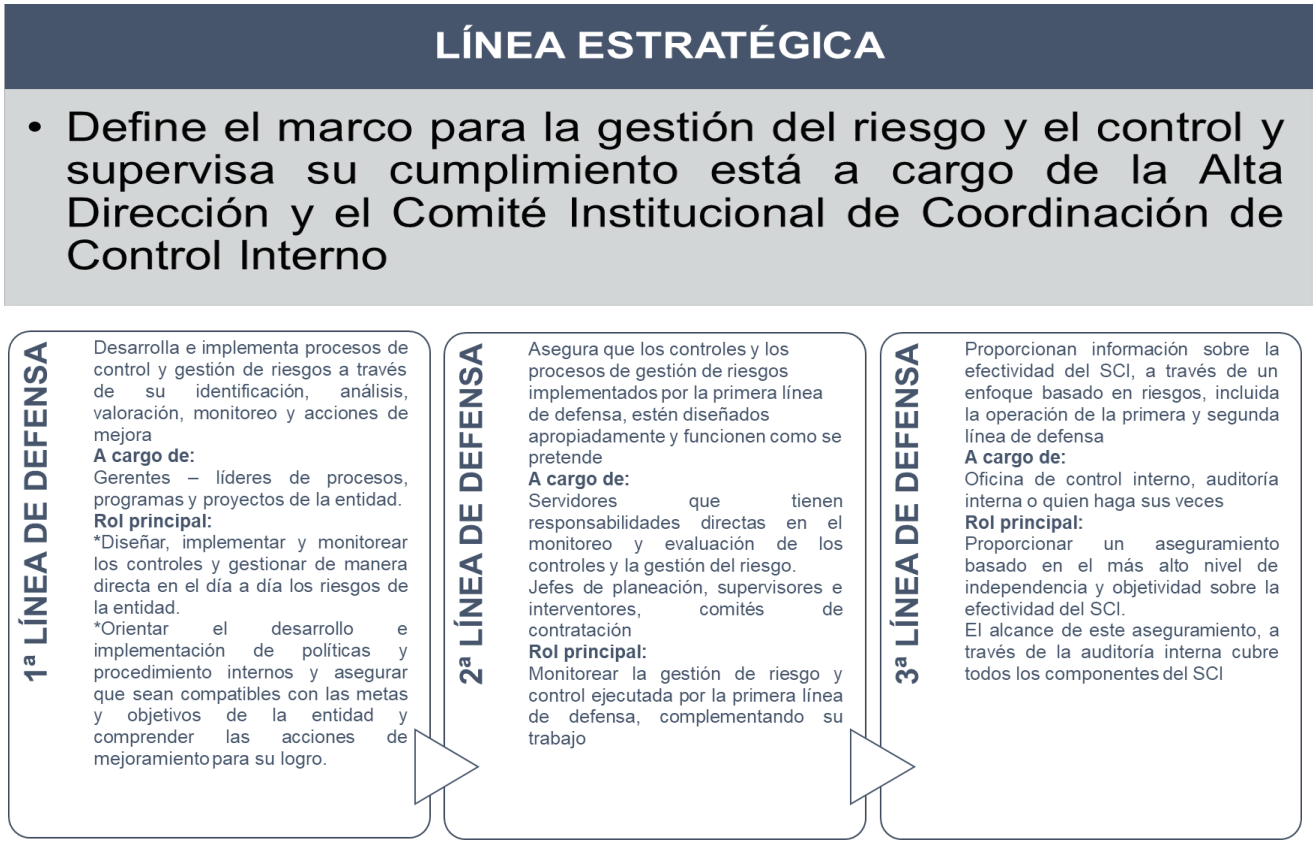
Hace referencia a una colección de datos históricos, por periodos de tiempo, relacionados con algún evento cuyo comportamiento puede indicar una mayor o menor exposición a determinados riesgos. No indica la materialización de los riesgos, pero sugiere que algo no funciona adecuadamente y, por lo tanto,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

Un indicador clave de riesgo, o KRI, por su sigla en inglés (Key Risk Indicators), permite capturar la ocurrencia de un incidente que se asocia a un riesgo identificado previamente y que es considerado alto, lo cual permite llevar un registro de ocurrencias y evaluar a través de su tendencia la eficacia de los controles que se disponen para mitigarlos.

10.5.Monitoreo y revisión

El modelo integrado de plantación y gestión (MIPG) desarrolla en la dimensión 7 control interno las líneas de defensa para identificar la responsabilidad de la gestión del riesgo y control que está distribuida en diversos servidores de la entidad como sigue:

Esquema de líneas de defensa



11.LINEAMIENTOS SOBRE LOS RIESGOS RELACIONADOS CON POSIBLES ACTOS DE CORRUPCIÓN

Para los riesgos asociados a posibles actos de corrupción se deben definir los lineamientos para su tratamiento. Es claro que este tipo de riesgos no admiten aceptación del riesgo; así mismo, se deben incluir las matrices relacionadas con la redacción de este tipo de riesgos, las preguntas para la definición del nivel de impacto y la matriz de calor correspondiente, donde se precisan las zonas de severidad aplicables. Para esta tipología de riesgos se incluye el protocolo para la identificación de riesgos de corrupción, asociados a corrupción.

11.1. RIESGO DE CORRUPCIÓN

Definición de 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 No. 167 de 2013).

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.

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.

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

De acuerdo con la siguiente matriz, si se marca con una X en la descripción del riesgo que aparece en cada casilla quiere decir que se trata de un riesgo de corrupción:

MATRIZ: DEFINICIÓN DEL RIESGO DE CORRUPCIÓN				
Descripción del riesgo	**Acción u omisión**	**Uso del poder**	**Desviar la gestión de lo público**	**Beneficio privado**

Generalidades acerca de los riesgos de corrupción
- Entidades encargadas de gestionar el riesgo: lo deben adelantar las entidades del orden nacional, departamental y municipal.

- Se elabora anualmente por cada responsable de los procesos al interior de las entidades junto con su equipo.

- Consolidación: la oficina de planeación, quien haga sus veces, o a la de dependencia encargada de gestionar el riesgo le corresponde liderar el proceso de administración de estos. Adicionalmente, esta misma oficina será la encargada de consolidar el mapa de riesgos de corrupción.

Publicación del mapa de riesgos de corrupción: se debe publicar en la página web de la entidad, en la sección de transparencia y acceso a la información pública que establece el artículo 2.1.1.2.1.4 del Decreto 1081 de 2015 o en un medio de fácil acceso al ciudadano, a más tardar el 31 de enero de cada año.

La publicación será parcial y fundamentada en la elaboración del índice de información clasificada y reservada. En dicho instrumento la entidad debe establecer las condiciones de reserva y clasificación de algunos de los elementos constitutivos del mapa de riesgos en los términos dados en los artículos 18 y 19 de la Ley 1712 de 2014.

En este caso se deberá anonimizar esa información. Es decir, la parte clasificada o reservada, aunque se elabora, no se hace visible en la publicación.

Recuerde que las excepciones solo pueden estar establecidas en la ley, un decreto con fuerza de ley o un tratado internacional ratificado por el Congreso o en la Constitución.

- Socialización: Los servidores públicos y contratistas de la entidad deben conocer el mapa de riesgos de corrupción antes de su publicación. Para lograr este propósito la oficina de planeación o quien haga sus veces, o la de gestión del riesgo deberá diseñar y poner en marcha las actividades o mecanismos necesarios para que los funcionarios y contratistas conozcan, debatan y formulen sus apreciaciones y propuestas sobre el proyecto del mapa de riesgos de corrupción.

Así mismo, dicha oficina adelantará las acciones para que la ciudadanía y los interesados externos conozcan y manifiesten sus consideraciones y sugerencias sobre el proyecto del mapa de riesgos de corrupción. Deberá dejarse la evidencia del proceso de socialización y publicarse sus resultados.

- Ajustes y modificaciones: se podrán llevar a cabo los ajustes y modificaciones necesarias orientadas a mejorar el mapa de riesgos de corrupción después de su publicación y durante el respectivo año de vigencia. En este caso deberán dejarse por escrito los ajustes, modificaciones o inclusiones realizadas.

- Monitoreo: en concordancia con la cultura del autocontrol al interior de la entidad, los líderes de los procesos junto con su equipo realizarán monitoreo y evaluación permanente a la gestión de riesgos de corrupción.

- Seguimiento: el jefe de control interno o quien haga sus veces debe adelantar seguimiento a la gestión de riesgos de corrupción. En este sentido es necesario que en sus procesos de auditoría interna analice las causas, los riesgos de corrupción y la efectividad de los controles incorporados en el mapa de riesgos de corrupción.

IMPORTANTE
Los riesgos de corrupción siempre deben gestionarse

IMPORTANTE
En la descripción de los riesgos de corrupción deben concurrir TODOS los componentes de su definición
ACCIÓN U OMISIÓN + USO DEL PODER + DESVIACIÓN DE LA GESTIÓN DE LO

Valoración de riesgos
Cálculo de la probabilidad e impacto

Análisis de la probabilidad
Se analiza qué tan posible es que ocurra el riesgo, se expresa en términos de frecuencia o factibilidad, donde frecuencia implica analizar el número de eventos en un periodo determinado, se trata de hechos que se han materializado o se cuenta con un historial de situaciones o eventos asociados al riesgo; factibilidad implica analizar la presencia de factores internos y externos que pueden propiciar el riesgo, se trata en este caso de un hecho que no se ha presentado, pero es posible que suceda.

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

Análisis del impacto

El impacto se debe analizar y calificar a partir de las consecuencias identificadas en la fase de descripción del riesgo

Criterios para calificar el impacto en riesgos de corrupción

Criterios para calificar el Impacto – Riesgos de Corrupción

Nro	PREGUNTA: Si el riesgo de corrupción se materializa podría...	Respuesta SI	Respuesta 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 o servicios o los 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	¿Genera daño ambiental		X
Responder afirmativamente de UNO a CINCO pregunta(s) genera un impacto **Moderado**. Responder afirmativamente de SEIS a ONCE preguntas genera un impacto **Mayor**. Responder afirmativamente de DOCE a DIECIOCHO preguntas genera un impacto **Catastrófico**.		10	
MODERADO	Genera medianas consecuencias sobre la entidad		
MAYOR	Genera altas consecuencias sobre la entidad.		
CATASTROFICO	Genera consecuencias desastrosas para la entidad		

Nivel de Impacto **MAYOR**

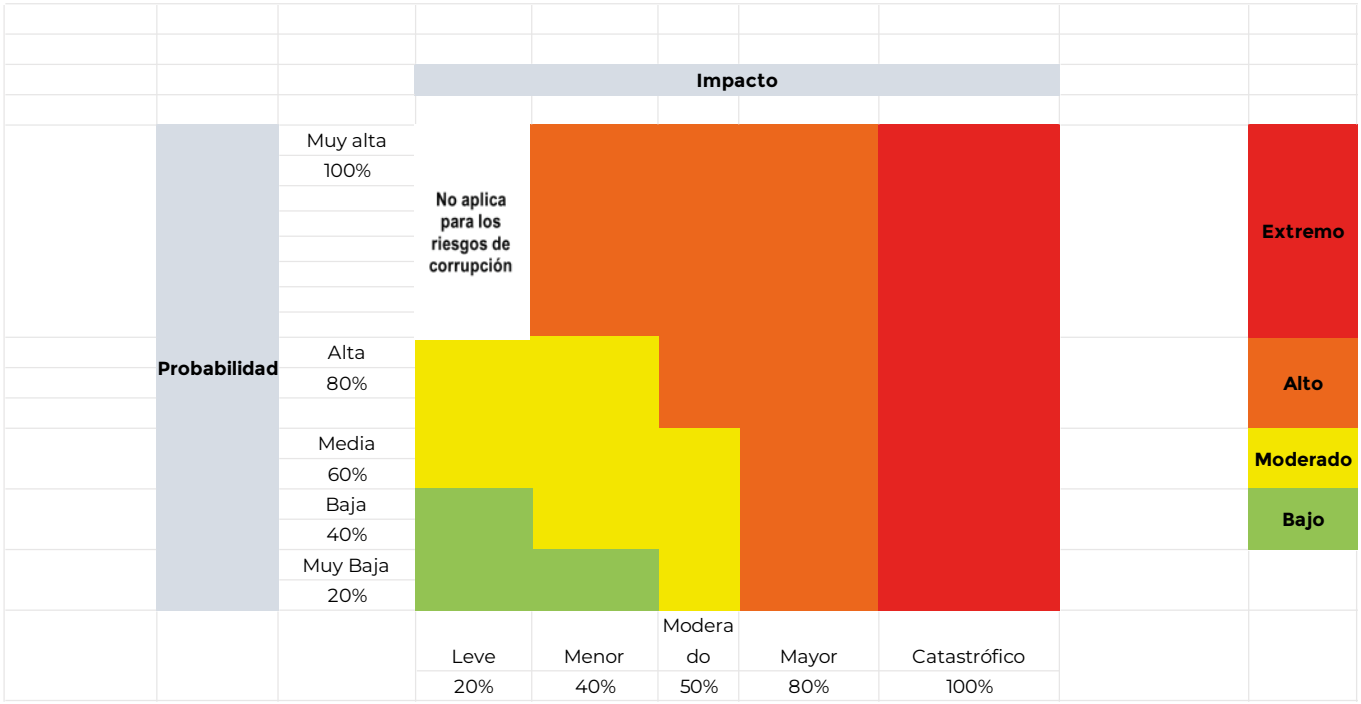
IMPORTANTE
Si la respuesta a la pregunta 16 es afirmativa, el riesgo se considera catastrófico.
Por cada riesgo de corrupción identificado se debe diligenciar una tabla de estas

Análisis del impacto en riesgos de corrupción

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

Por último, ubique en el mapa de calor el punto de intersección resultante de la probabilidad y el impacto para establecer el nivel del riesgo inherente.

IMPORTANTE
Aunque se utilice el mismo mapa de calor, para los riesgos de gestión y corrupción, a estos últimos solo se les aplican las columnas de impacto



Valoración de los controles – diseño de controles

Tenga en cuenta para el diseño de controles, los parámetros señalados en la versión 4 de la Guía para la administración del riesgo y el diseño de controles en entidades públicas, de 2018, continúan vigentes, por lo tanto se sugiere remitirse a dicho documento.

Nivel del riesgo (riesgo residual)

Desplazamiento del riesgo inherente para calcular el riesgo residual

IMPORTANTE
Tratándose de riesgos de corrupción únicamente hay disminución de probabilidad. Es decir, para el impacto

Tratamiento del riesgo

¿Qué es tratamiento del riesgo?

Es la respuesta establecida por la primera línea de defensa para la mitigación de los diferentes riesgos, incluyendo aquellos relacionados con la corrupción. A la hora de evaluar las opciones existentes en materia de tratamiento del riesgo, y partiendo de lo que establezca la política de administración del riesgo, los dueños de los procesos tendrán en cuenta la importancia del riesgo, lo cual incluye el efecto que puede tener sobre la entidad, la probabilidad e impacto de este y la relación costo-beneficio de las medidas de tratamiento. Pero en caso de que una respuesta ante el riesgo derive en un riesgo residual que supere los niveles aceptables para la dirección se deberá volver a analizar y revisar dicho tratamiento. En todos los casos para los riesgos de corrupción la respuesta será evitar, compartir o reducir el riesgo. El tratamiento o respuesta dada al riesgo, se enmarca en las siguientes categorías:

ACEPTAR EL RIESGO

IMPORTANTE
En el caso de riesgos de corrupción, estos no pueden

EVITAR EL RIESGO

Cuando los escenarios de riesgo identificado se consideran demasiado extremos se puede tomar una decisión para evitar el riesgo, mediante la cancelación de una actividad o un conjunto de actividades.

Desde el punto de vista de los responsables de la toma de decisiones, este tratamiento es simple, la menos arriesgada y menos costosa, pero es un obstáculo para el desarrollo de las actividades de la entidad y, por lo tanto, hay situaciones donde no es una opción.

COMPARTIR EL RIESGO

Cuando es muy difícil para la entidad reducir el riesgo a un nivel aceptable o se carece de conocimientos necesarios para gestionarlo, este puede ser compartido con otra parte interesada que pueda gestionarlo con más eficacia. Cabe señalar que normalmente no es posible transferir la responsabilidad del riesgo.

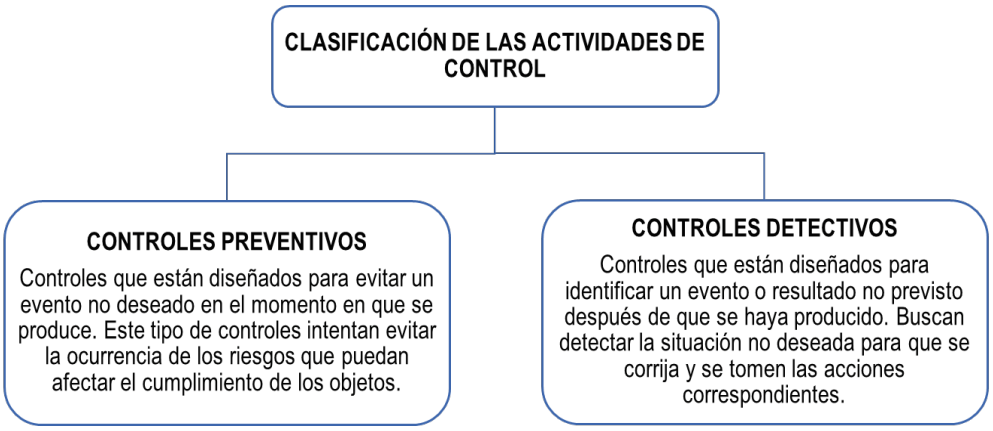
REDUCIR EL RIESGO

El nivel de riesgo debería ser administrado mediante el establecimiento de controles, de modo que el riesgo residual se pueda reevaluar como algo aceptable para la entidad.

Estos controles disminuyen normalmente la probabilidad y/o el impacto del riesgo.

Deberían seleccionarse controles apropiados y con una adecuada segregación de funciones, de manera que el tratamiento al riesgo adoptado logre la reducción prevista sobre este.

Tratamiento del riesgo – rol de la primera línea de defensa
Como medio para propiciar el logro de los objetivos, las actividades de control se orientan a prevenir y detectar la materialización de los riesgos. Por consiguiente, su efectividad depende, de qué tanto se están logrando los objetivos estratégicos y de proceso de la entidad. Le corresponde a la primera línea de defensa el establecimiento de actividades de control.



Monitoreo de riesgos de corrupción
Los gerentes públicos 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), para este propósito se sugiere elaborar una matriz. Dicho monitoreo será en los tiempos que determine la entidad.

Su importancia radica en la necesidad de llevar a cabo un seguimiento constante a la gestión del riesgo y a la efectividad de los controles establecidos. Teniendo en cuenta que la corrupción es, por sus propias características, una actividad difícil de detectar.

Para tal efecto deben atender a los lineamientos y las actividades descritas en la primera y segunda línea de defensa de este documento.

Reporte de la gestión del riesgo de corrupción
De igual forma, se debe reportar en el mapa y plan de tratamiento de riesgos los riesgos de corrupción, de tal manera que se comunique toda la información necesaria para su comprensión y tratamiento adecuado.

Seguimiento de riesgos de corrupción

GESTIÓN RIESGOS DE CORRUPCIÓN
* Seguimiento: El Jefe de Control Interno o quien haga sus veces, debe adelantar seguimiento al Mapa de Riesgos de Corrupción. En este sentido es necesario que adelante seguimiento a la gestión del riesgo, verificando la efectividad de los controles.

* 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. (Anexo: matriz de seguimiento a los riesgos de corrupción)

En especial deberá adelantar las siguientes actividades:

- Verificar la publicación del Mapa de Riesgos de Corrupción en la página web de la entidad.
- Seguimiento a la gestión del riesgo.
- Revisión de los riesgos y su evolución.
- Asegurar que los controles sean efectivos, le apunten al riesgo y estén funcionando en forma adecuada.

Acciones a seguir en caso de materialización de riesgos de corrupción
En el evento de materializarse un riesgo de corrupción, es necesario realizar los ajustes necesarios con acciones, tales como:
1) Informar a las autoridades de la ocurrencia del hecho de corrupción.
2) Revisar el mapa de riesgos de corrupción, en particular, las causas, riesgos y controles.
3) Verificar si se tomaron las acciones y se actualizó el mapa de riesgos de corrupción.
4) Llevar a cabo un monitoreo permanente.

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

Las acciones adelantadas se refieren a:

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

12.Lineamientos 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.

12.1.Identificación de los activos de seguridad de la información

Como primer paso para la identificación de riesgos de seguridad de la información es necesario identificar los activos de información del proceso.

Conceptualización activos de información:

¿Qué son los activos?	¿Por qué identificar los activos?
• 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 • Redes • Información física o digital • Tecnologías de la información TI • Tecnologías de operación TO que utiliza la organización para funcionar en el entorno digital	• Permite determinar que es lo más importante en cada entidad y sus procesos poseen (sean bases de datos, archivos, servidores web o aplicaciones clave para que la entidad pueda prestar sus servicios. • 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.

¿Cómo identificar los activos?

Proceso	Activo	Descripción	Dueño del activo	Tipo del activo	Ley 1712 de 2014	Ley 1581 de 2012	Criticidad respecto a su confidencialidad	Criticidad respecto a completitud o integridad	Criticidad respecto a su disponibilidad	Nivel de criticidad

12.2.Identificación del riesgo

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

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

Para cada riesgo se deben asociar el grupo de activos, o activos específicos del proceso, y conjuntamente analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización. Para este efecto, es necesario consultar el Anexo Modelo nacional de gestión de riesgos de seguridad de la información para entidades públicas donde se encuentran las siguientes tablas necesarias para este análisis:

- Tabla 5. Tabla de amenazas comunes
- Tabla 6. Tabla de amenazas dirigida por el hombre
- Tabla 7. Tabla de vulnerabilidades comunes

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.

Tipo de activo	Vulnerabilidades	Amenazas

Formato de descripción del riesgo de seguridad de la información

Riesgo	Activo	Descripción del riesgo	Amenaza	Tipo	Causas / Vulnerabilidades	Consecuencias
					(Seleccionar las vulnerabilidades asociadas a la amenaza identificada)	

IMPORTANTE

* Existirían tres (3) tipos de riesgos: pérdida de confidencialidad, pérdida de la integridad y pérdida de la disponibilidad de los activos. Para cada tipo de riesgo se podrán seleccionar las amenazas y las vulnerabilidades que puedan causar que dicho riesgo se materialice.
* Los catálogos de amenazas y vulnerabilidades comunes se encuentran en la sección 4.1.7. del **anexo "Lineamientos para la gestión del riesgo de seguridad digital en entidades públicas"**, el cual hace parte de la presente guía.
* **NOTA 1:** tener en cuenta que la agrupación de activos debe ser del mismo tipo, por ejemplo, analizar conjuntamente activos tipo hardware, software, información, entre otros, para determinar amenazas y vulnerabilidades comunes que puedan afectar a dicho grupo.
* **NOTA 2:** las entidades públicas deben incluir como mínimo los procesos y procedimientos establecidos en esta guía. Aquellas entidades que ya estén adelantando procesos relacionados con la gestión de este tipo de riesgo y que incorporen al menos lo dispuesto en estas guías podrán continuar bajo sus procedimientos. Si alguno de los aspectos contenidos en esta guía no está contemplado, deberá ser agregado a los que manejan actualmente.

12.3.Valoración del riesgo

Para esta etapa se asociarán las tablas de probabilidad e impacto definidas en la primera parte de la presente guía.

	Frecuencia de la Actividad	Probabilidad
Muy baja	La actividad que conlleva el riesgo se ejecuta como máximo 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%

La determinación del impacto se debe llevar a cabo de acuerdo con lo establecido en la presente guía, entendiendo que el impacto se entiende como la consecuencia económica y reputacional que se genera por la materialización del riesgo.

Leve 20%	Afectación menor a 10 SMLVM	El riesgo afecta la imagen de algún área de la organización
Menor 40%	Entre 10 y 50 SMLVM	El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, de junta directiva y accionistas y/o proveedores
Moderado 60%	Entre 50 y 100 SMLVM	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 SMLVM	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 SMLVM	El riesgo afecta la imagen a nivel nacional, con efecto publicitario sostenido a nivel país

Para el análisis preliminar (riesgo inherente), en esta etapa se define el nivel de severidad para el riesgo de seguridad de la información identificado, para ello, se aplica la matriz de calor establecida.

		Impacto						
Probabilidad	Muy alta							Extremo
	100%							
	Alta							Alto
	80%							
	Media							Moderado
	60%							
	Baja							Bajo
	40%							
	Muy Baja							
	20%							
		Leve	Menor	Moderado	Mayor	Catastrófico		
		20%	40%	50%	80%	100%		

Valoración del riesgo en seguridad de la información

IMPORTANTE
Cada entidad deberá adaptar los criterios a su realidad.
El nivel de impacto deberá ser determinado con la presencia de cualquiera de los criterios establecidos, tomando el criterio con mayor

Las variables de confidencialidad, integridad y disponibilidad se definen de acuerdo con el modelo de seguridad y privacidad de la información de la estrategia de Gobierno Digital del MINTIC

La variable población se define teniendo en cuenta el establecimiento del contexto externo de la entidad, es decir, que la consideración de la población va a estar asociada a las personas a las cuales se les prestan los servicios o trámites en el entorno digital y que de una u otra forma pueden verse afectadas por la materialización de algún riesgo en los activos identificado. Los porcentajes en las escalas pueden variar, según la entidad y su contexto.

La variable presupuesto es la consideración de presupuesto afectado por la entidad debido a la materialización del riesgo, contempla sanciones económicas o impactos directos en la ejecución presupuestal

Riesgo	Activo	Amenaza	Vulnerabilidad	Probabilidad	Impacto	Zona de riesgo
						Extremo
						Alto
						Moderado
						Bajo

IMPORTANTE
La probabilidad y bel impacto se determinan con base a la amenaza no en las vulnerabilidades

La variable ambiental estará también alineada con la afectación del medio ambiente por la materialización de un riesgo de seguridad digital. Esta variable puede no ser utilizada en la mayoría de los casos, pero debe tenerse en cuenta, ya que en alguna eventualidad puede existir afectación ambiental

12.4.Controles asociados a la seguridad de la información

Las entidades públicas podrán mitigar/tratar los riesgos de seguridad de la información empleando como mínimo los controles del Anexo A de la ISO/IEC 27001:2013, estos controles se encuentran en el anexo 4. "Modelo Nacional de Gestión de riesgo de seguridad de la Información en entidades públicas", siempre y cuando se ajusten al análisis de riesgos.

Acorde con el control seleccionado, será necesario considerar las características de diseño y ejecución definidas para su valoración.

No.	RIESGO	ACTIVO	TIPO	AMENAZAS	TIPO	PROBABILIDAD	IMPACTO	RIESGO RESIDUAL	OPCION TRATAMIENTO	ACTIVIDAD DE CONTROL	SOPORTE	RESPONSABLE	TIEMPO	INDICADOR

telecafé

Expresión de lo nuestro

Política de Operación para la Administración del Riesgo en Telecafé LTDA

www.telecafe.gov.co

@canaltelecafe