

Versión	fecha	Descripción
2	Noviembre 2018	Se incluye la definición y alcance
3	Enero 31 de 2022	La resolución por la cual se adopta la gestión de riesgo, se actualiza la metodología según la guía del DAFP.
4	Marzo 25 de 2022	Se actualiza el documento, con el fin de establecer dentro del alcance, la identificación de los riesgos operativos relacionados con SG-SST y Gestión ambiental en cada uno de los procesos del SIG.
5	Octubre de 2024	Se actualiza teniendo en cuenta auditoria externa 2023, en la cual se debe incluir la evaluación de la eficacia de los controles.

Definición

La presente guía define los lineamientos que deben seguir los procesos para la identificación, análisis y valoración de los riesgos (eventos negativos internos y externos que puedan afectar o impedir el logro de la misión y los objetivos institucionales) durante el desarrollo de las actividades de acuerdo con el objetivo del mismo.

Adicionalmente, permite orientar la definición de las acciones correspondientes, que deben establecer cada uno de los procesos con el fin de prevenir y mitigar los riesgos y así enfocar los esfuerzos a la mejora continua de la gestión, estableciendo responsabilidades y seguimiento a estas acciones a través de los planes de acción y la evaluación de la eficacia de los controles establecidos.



Alcance

Aplica a todos los procesos del Sistema Integrado de Gestión SIG. Inicia con la identificación del riesgo, de acuerdo con el objetivo de cada proceso y termina con el seguimiento al plan de acción. Lo anterior de acuerdo con los parámetros establecidos en la norma NTC-ISO 9001:2015 en el numeral 6.1. Así mismo, se deben determinar los riesgos operativos asociados con SG-SST y Gestión ambiental, los cuales se deben identificar para cada proceso del sistema.

Generalidades

Para llevar a cabo la identificación, análisis y valoración del riesgo dentro de cada uno de los procesos, se determinó el contexto en la UPTC, el cual se basa en un modelo de análisis de riesgo, establecido por el consejo superior con apoyo de la rectoría y el proceso de planeación institucional.

En este diagnóstico se incluyen las cuestiones de los procesos y los requisitos de las partes interesadas, dicho diagnóstico es aprobado por el consejo Superior según las estancias administrativas de la Universidad.

El contexto es documentado en el plan Maestro institucional y acotado en el Plan de desarrollo institucional, en periodos establecidos de tiempo (no mayor a 4 años, que es el período de gestión y labor operativa del rector) y el Plan de Acción (con seguimiento anual).

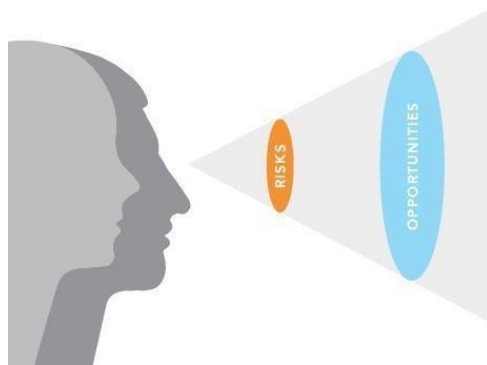
Gestión de las cuestiones y acciones para abordar riesgos y oportunidades.

Identificación de cuestiones: La determinación de cuestiones se da por consulta a cada uno de los procesos, teniendo en cuenta aquellas situaciones que pueden afectar los resultados esperados del sistema integrado de gestión o aquellas situaciones que puedan potenciar el aumento en la satisfacción del cliente y la mejora en el desempeño ambiental.



Acciones para abordar riesgos y oportunidades.

La gestión de las cuestiones se realizará según las directrices administrativas que determina la gestión pública. Para la Universidad Pedagógica y Tecnológica de Colombia se seleccionaron las siguientes dos metodologías para gestionar las cuestiones:



- **Gestión de los riesgos:** la gestión de los riesgos se administrará según la guía metodológica de gestión del riesgo determinada por el Departamento administrativo de la función pública según la versión vigente en que se encuentre el documento oficial. En esta guía se establecen los métodos para gestionar los riesgos de tal manera que las partes interesadas sean respetadas y se dé cumplimiento a sus requisitos. Así mismo sin afectar la coordinación, operación e integridad de la entidad pública donde se aplica.

La universidad pedagógica y tecnológica de Colombia, por medio de la resolución 4843 de 2021, adopta la Política para la administración del Riesgo de Gestión, Corrupción y Seguridad Digital y se deroga la resolución 4256 de 2010. Es así que se realizaron actividades con cada uno de los procesos y se diligencio la matriz estandarizada por el DAFP, para la gestión de los riesgos operativos.

Gestión de las oportunidades: La Universidad Pedagógica y Tecnológica de Colombia ha determinado que la gestión de las oportunidades se realizará, desde su determinación hasta su seguimiento y verificación de eficacia, por medio de la aplicación



de planes de acción. Metodología definida por el área de planeación institucional y en operación por el área de planeación y de control interno.

Monitoreo y Revisión del Riesgo

Con el establecimiento del Taller de Evaluación de la Gestión, los líderes de proceso junto con sus equipos de trabajo deben monitorear y revisar trimestralmente los factores críticos de los procesos, detectar desviaciones y permitir establecer las medidas correctivas que garanticen la continuidad de la operación y satisfacción de los objetivos de la entidad.

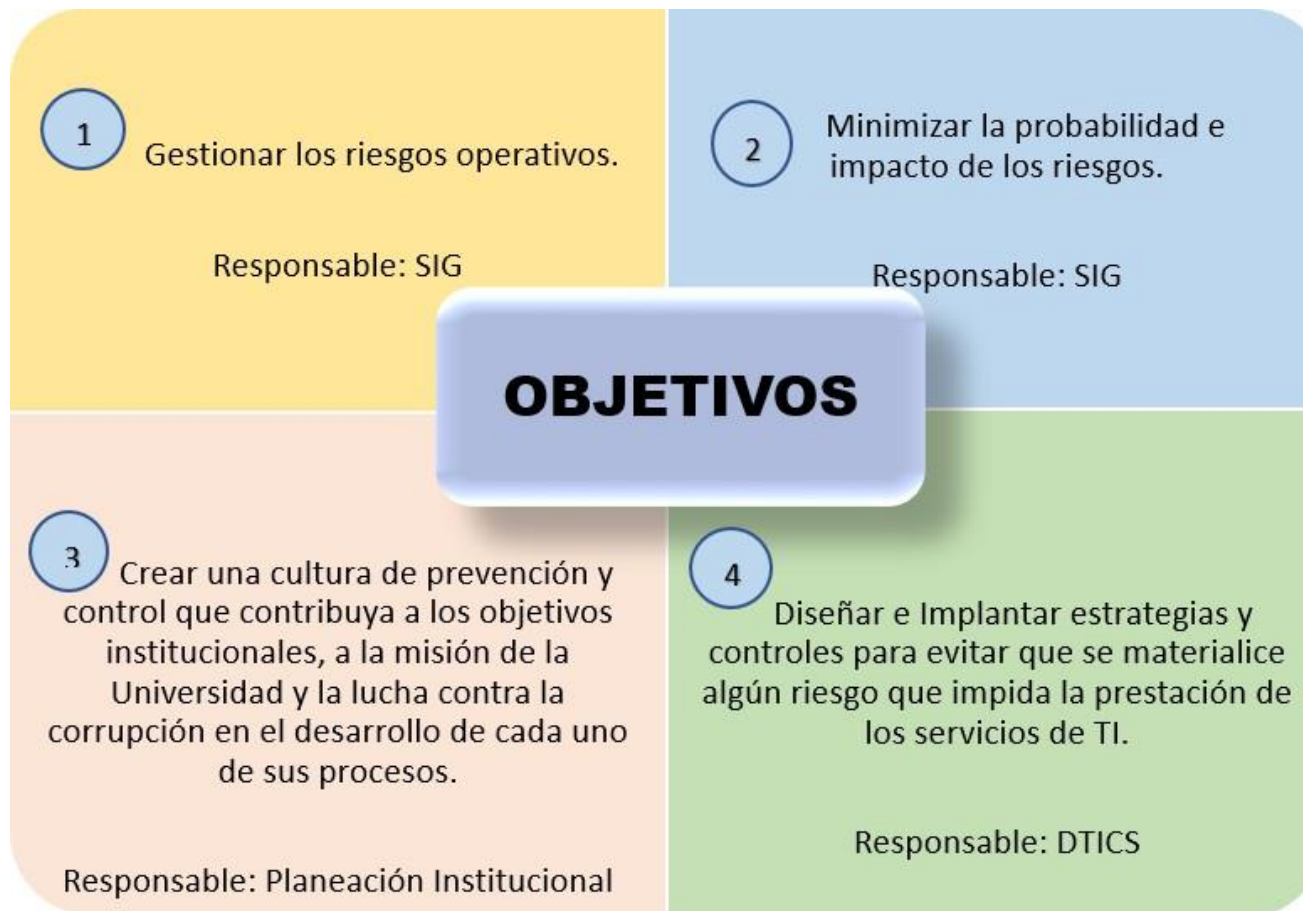
En el Numeral 4 del orden del día, se hará el correspondiente análisis del riesgo, determinar si los controles han sido efectivos o si es necesario generar más acciones.

Seguimiento

Una vez el proceso apruebe las acciones necesarias para mitigar el riesgo en la matriz, se tendrán en cuenta las fechas de seguimiento establecidas, posteriormente el proceso de Evaluación Independiente hará el respectivo seguimiento al cumplimiento de las acciones formuladas.

1. POLÍTICA PARA LA ADMINISTRACIÓN DEL RIESGO DE GESTIÓN, CORRUPCIÓN Y SEGURIDAD DIGITAL DE LA UNIVERSIDAD PEDAGÓGICA Y TECNOLÓGICA DE COLOMBIA.

La Universidad Pedagógica y Tecnológica de Colombia se compromete a adoptar los mecanismos para crear una cultura en la gestión integral de los riesgos, definiendo esquemas, optimizando procesos y procedimientos y estableciendo los lineamientos para la actualización de la metodología con el fin de identificar, priorizar y valorar los riesgos propios de su actividad, que puedan afectar el cumplimiento de su función constitucional, los objetivos, la misión, los planes y proyectos institucionales. Así mismo se compromete a preservar la confidencialidad, disponibilidad e integridad, de sus activos de información.



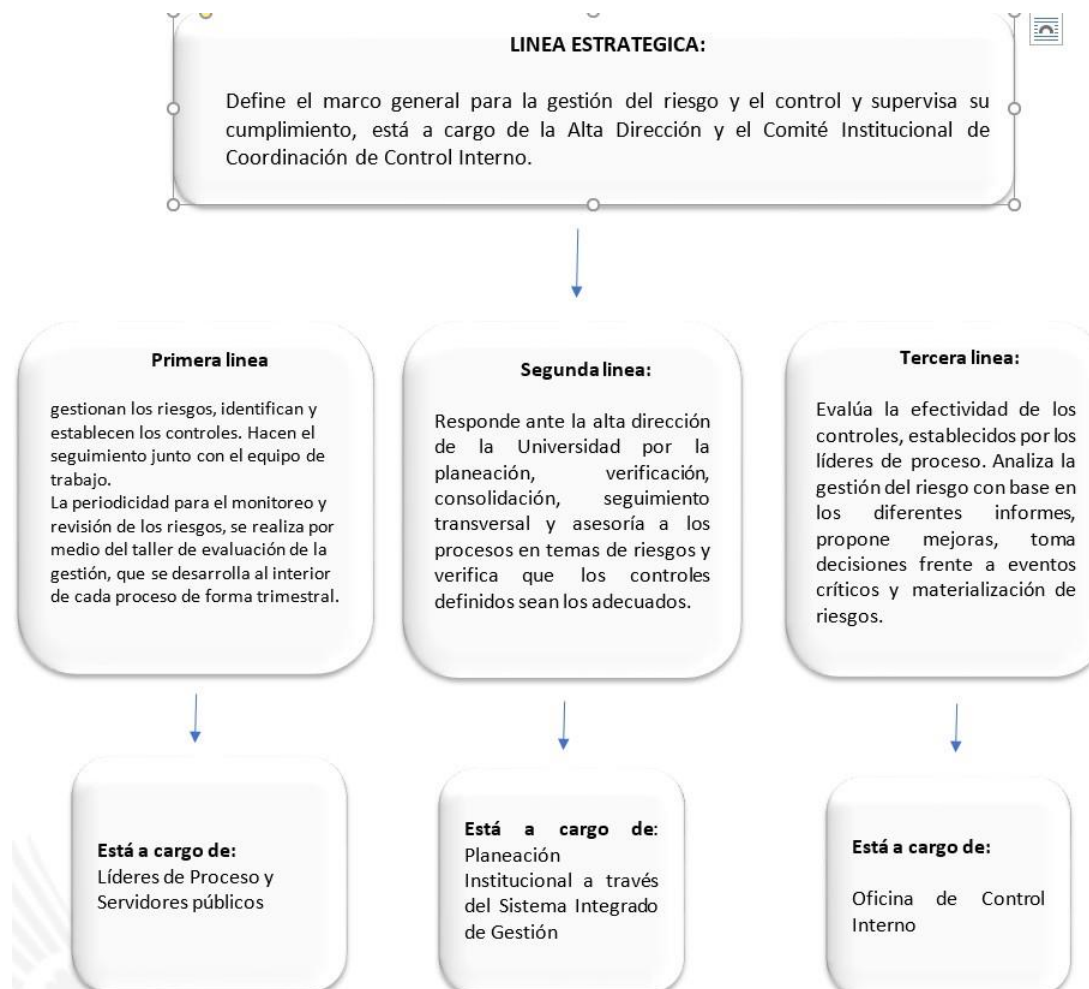
1. ALCANCE:

La política de Administración del Riesgo de Gestión, Corrupción y Seguridad Digital aprobada en la presente resolución, será de aplicación general para todos los procesos del Sistema Integrado de Gestión de la UPTC.

1. AUTORIDADES Y RESPONSABILIDADES:

Definir los niveles de autoridad y responsabilidad para la administración del riesgo.

Para la adecuada gestión del riesgo se han definido las siguientes líneas de operatividad institucional:



4. CONCEPTOS BÁSICOS RELACIONADOS CON LA GESTIÓN DEL RIESGO

- **Riesgo:** Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales.

Nota: Los 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 eventos.

- **Riesgo Inherente:** Es un riesgo sin controles, el resultado de combinar la probabilidad con el impacto, nos permite determinar el nivel del riesgo inherente, dentro de unas escalas de severidad.
- **Riesgo Residual:** El resultado de aplicar la efectividad de los controles al riesgo inherente.
- **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.
- **Impacto:** las consecuencias que puede ocasionar a la organización la materialización del riesgo.
- **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.
- **Factores de Riesgo:** Son las fuentes generadoras de riesgos.
- **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. El control establecido debe atacar la causa raíz.



- **Factores de Riesgo:** Son las fuentes generadoras de riesgos.
- **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.
- **Confidencialidad:** Propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados.
- **Integridad:** Propiedad de exactitud y completitud.
- **Disponibilidad:** Propiedad de ser accesible y utilizable a demanda por una entidad.

2. METODOLOGÍA

La metodología a utilizar será la establecida por el Departamento Administrativo de la Función Pública en la Guía para la administración del Riesgo y el Diseño de Controles en Entidades Públicas- versión 5 de 2020.

5.1. Identificación del riesgo:

El objetivo es identificar los riesgos que estén o no bajo el control de la Universidad, para ello se tendrá en cuenta el contexto estratégico y la caracterización de los procesos.

1

Análisis de los objetivos estratégicos y de los procesos: Se deben analizar los objetivos establecidos en el plan de desarrollo institucional y la caracterización de los procesos e identificar los posibles riesgos que afecten su cumplimiento.

2

Identificación de los puntos de Riesgo: Dentro del flujo de actividades de los procesos, existen evidencias de que pueden ocurrir eventos de riesgo operativo y deben mantenerse bajo control, para asegurar que los procesos cumplan su objetivo

3

Identificación de áreas de impacto: Es la consecuencia económica o reputacional a la cual se ve expuesta la Universidad en caso de materializarse un riesgo. Los impactos que aplican son afectación económica (o presupuestal) y reputacional

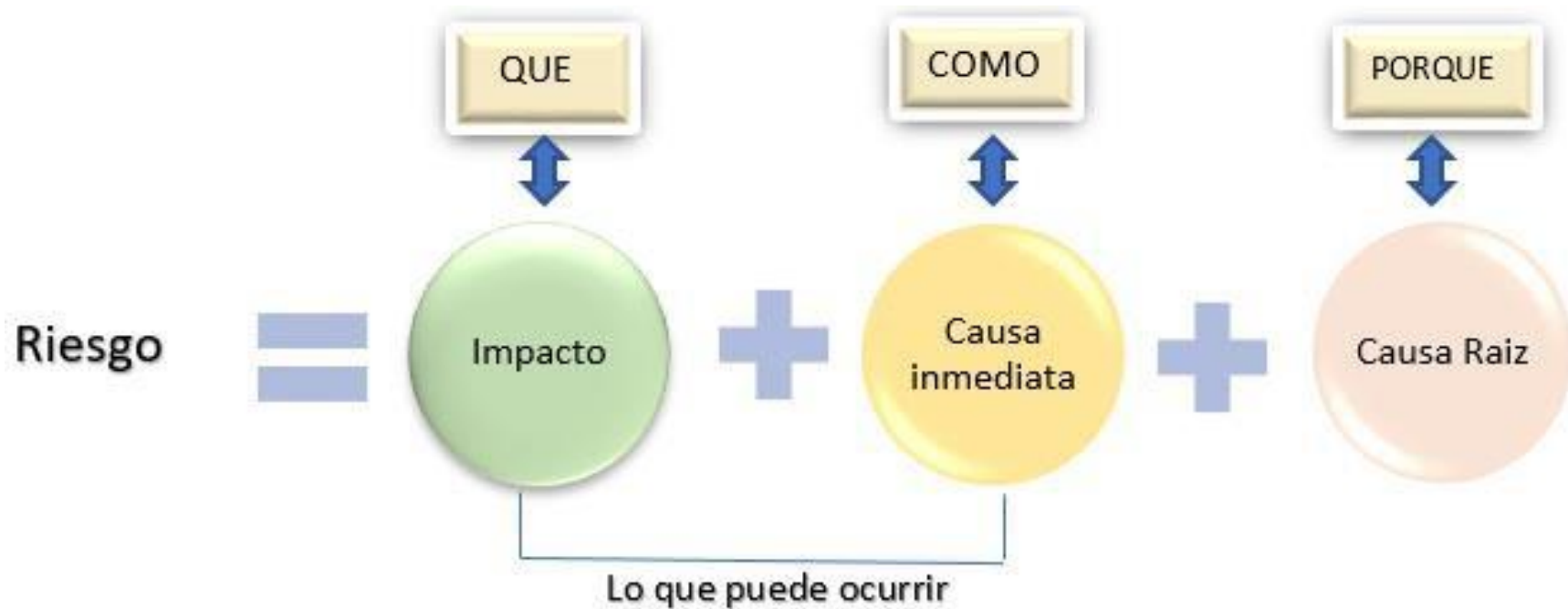
4

Identificación de áreas de factores de riesgo: Se deben identificar y analizar las fuentes generadoras de riesgos (procesos, tecnología, Infraestructura, eventos externos, talento humano).

5

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:



- **Impacto:** Las consecuencias que puede ocasionar a la organización la materialización del riesgo.
- **Causa Inmediata:** Situaciones más evidentes sobre las cuales se presenta el riesgo, las mismas no constituyen la causa principal o base para para que se presente el riesgo.
- **Causa Raíz:** Es la causa principal o básica, corresponden a las razones por las cuales se puede presentar el riesgo, son la base para la definición de controles en la etapa de valoración del riesgo.



La anterior estructura evita la subjetividad en la redacción y permite entender la forma como se puede manifestar el riesgo, así como sus causas inmediatas y causas principales o raíz, esta es información esencial para la definición de controles en la etapa de valoración del riesgo.

5.2. Clasificación 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.

5.3. Valoración del riesgo

- **Análisis de riesgos:** En esta etapa se busca establecer la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto y se asocian los controles para su tratamiento.
- **Probabilidad:** Se basa en el número de veces en que se pasa por el punto de riesgo en el periodo de un año.

- **Impacto:** Consecuencias que puede ocasionar a la entidad por la materialización de un riesgo (reputacional y afectación económica), cuando se presenten ambos impactos de riesgo, tanto económico como reputacional, con diferente nivel, se debe tomar el nivel más alto.

Tabla 1 Mapa de calor de la frecuencia de la 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%

Fuente: DAFP



Tabla 2 Impacto, considerando la perdida reputacional y afectación económica o presupuestal.

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

Fuente: DAFP

5.1. Evaluación de Riesgos: A partir del análisis de la probabilidad de ocurrencia del riesgo y sus consecuencias o impactos, se busca determinar la zona de riesgo inicial. (RIESGO INHERENTE)

Tabla 3. Matriz de calor (niveles de severidad del riesgo)

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

Fuente: DAFP

6. Valoración de controles.

Para poder llegar al riesgo residual, se definen los controles que son las medidas que permiten reducir o mitigar el riesgo. Se debe tener en cuenta.

- La identificación de controles, se realiza a cada riesgo.
- Los responsables de implementar los controles son los líderes de proceso, con el apoyo del equipo de trabajo.

6.1. Responsables de ejecutar el control:

Identifica el cargo del servidor que ejecuta el control, generalmente son de tipo manual porque los aplicamos las personas, en caso de que sean controles automáticos se identificará el sistema que realiza la actividad.

- **Acción:** Se determina mediante verbos (verificar, cotejar, validar, comparar) que indican la acción que deben realizar como parte del control.



- **Complemento:** Corresponde a los detalles que permiten identificar claramente el objeto del control.
- **Plan de acción:** Adicional a los controles existentes, se debe adelantar el plan de acción, con el responsable de la ejecución, la fecha de ejecución, determino si fue eficaz, si el riesgo se materializo o no e incluir la oportunidad conforme a lo definido en el plan de desarrollo institucional.

6.2. Tipologías de Controles

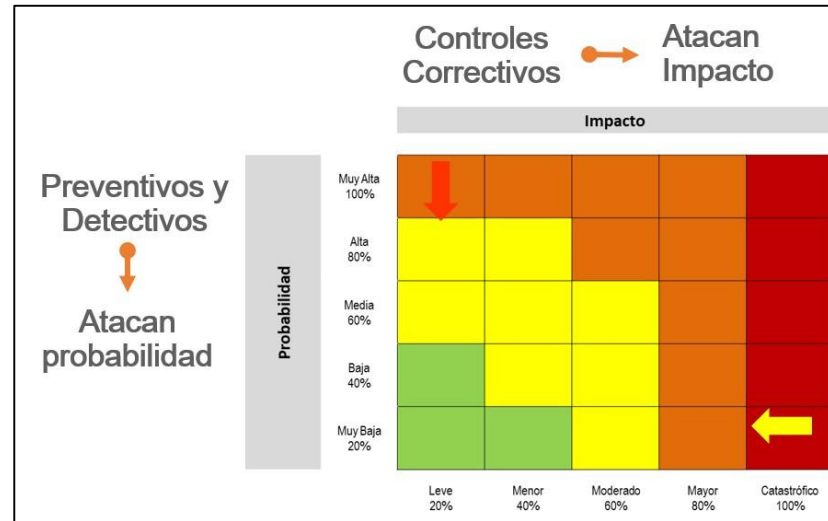
- **Control preventivo:** Va a las causas del riesgo, atacan la probabilidad de ocurrencia del riesgo, se acciona en la entrada del proceso, antes de que se realice la actividad originadora del riesgo. Busca establecer condiciones que aseguren el resultado esperado.
- **Control detectivo:** Detecta que algo ocurre y devuelve el proceso a los controles preventivos Atacan la probabilidad de ocurrencia del riesgo. Se acciona durante la ejecución del proceso, estos controles detectan el riesgo.
- **Control correctivo:** Atacan el impacto frente a la materialización del riesgo. Se acciona a la salida del proceso y después de que se materializa el riesgo.
- **Control manual:** Son ejecutados por personas.
- **Control automático:** Son ejecutados por un sistema.

Tabla 4. Análisis y evaluación de los controles – Atributos

		Características de Eficiencia		Peso
Eficiencia	Tipo	Preventivo		25%
		Detectivo		15%
		Correctivo		10%
	Implementación	Automático		25%
		Manual		15%
		Formalización del Control		**Nota Importante: Los atributos informativos solo permiten darle formalidad al control, 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.
Documentación	Documentado			
	Sin Documentar			
Frecuencia	Continua			
	Aleatoria			
Evidencia	Con Registro			
	Sin registro			
Atributos Informativos				

Fuente: DAFP

Tabla 5 Movimiento en la matriz de calor acorde con el tipo de control



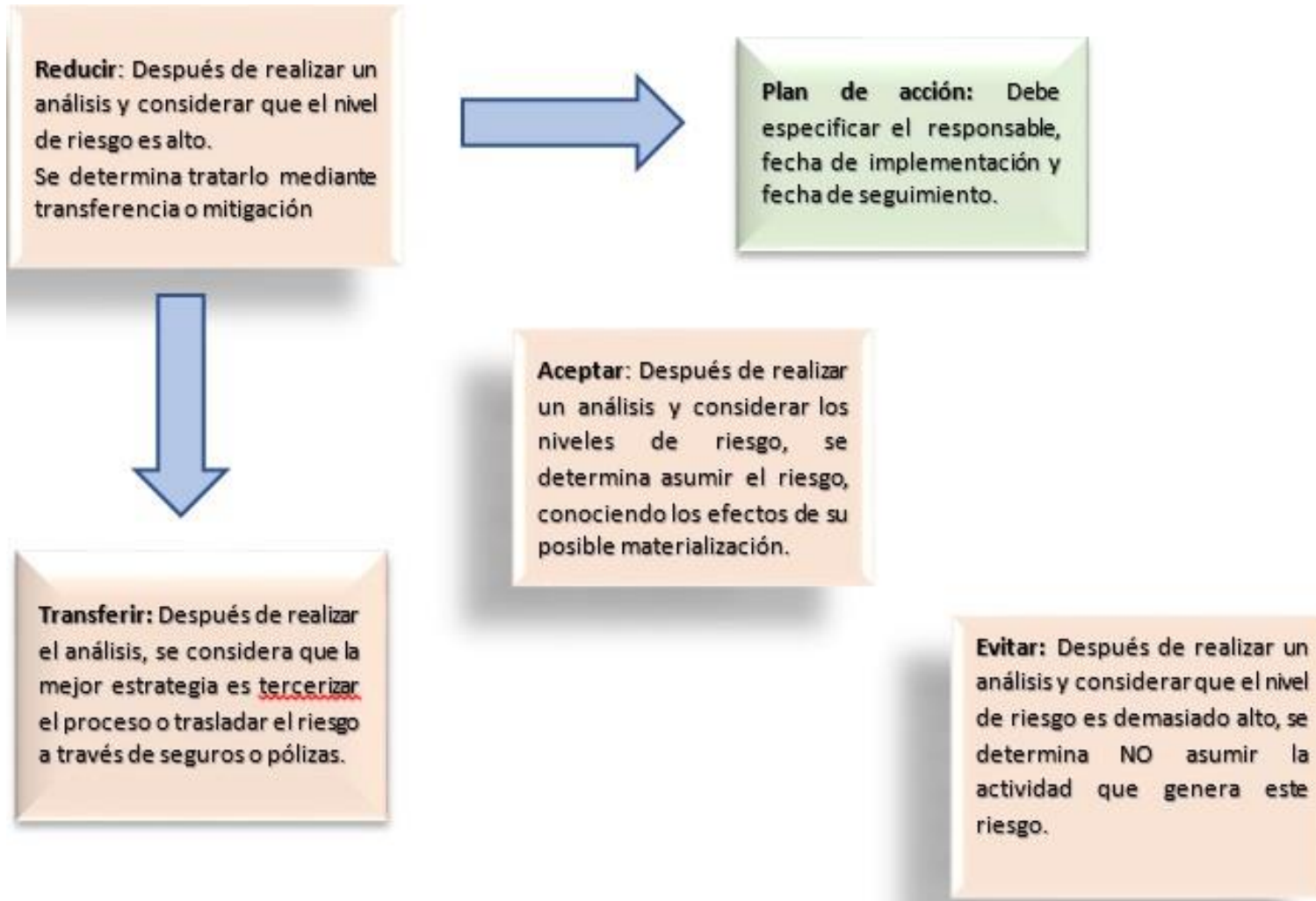
Fuente: DAFP

6.3. Nivel de Riesgo (Riesgo residual):

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

7. Estrategias para combatir el riesgo

Es la 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, procede a partir del riesgo inherente.





8. Estructura General de la Metodología para la Identificación, Valoración y Tratamiento de los riesgos seguridad en la información y los relacionados con posibles actos de corrupción.

De acuerdo con las políticas de transparencia, acceso a la información pública y lucha contra la corrupción liderada por la secretaría de transparencia y la de gobierno digital, se deben considerar los siguientes aspectos de acuerdo con los pasos de la metodología así:

8.1. Lineamientos sobre los riesgos relacionados con posibles actos de corrupción.

Para la gestión de riesgos de corrupción, la UPTC ha establecido los lineamientos para la administración del riesgo de corrupción, para lo cual adoptó las guías establecidas de la Presidencia de la República y el Departamento Administrativo de la Función Pública DAFP, como instrumento de tipo preventivo para analizar, valorar, tratar, comunicar, monitorear, revisar y realizar seguimiento a los mismos. Esta guía se encuentra disponible para su consulta, en el código de buen gobierno P-DS-C02.

9. Lineamientos para los riesgos de seguridad en la información

9.1. Identificación de los activos de seguridad en la información:

La Dirección de las Tecnologías y Sistemas de Información y de las Comunicaciones de la UPTC, mediante la implementación del sistema de gestión de seguridad de la información y la metodología para la gestión del riesgo, realiza la gestión de los riesgos de seguridad en la información. Los lineamientos se encuentran en el Plan de Gestión de Servicios de TI y de Seguridad de la Información, código A-RI-L03, así como el procedimiento Identificación, Clasificación y Gestión de Riesgos de Activos de Información, los procedimientos y guías asociadas al mismo.