MANUAL
GESTIÓN DE RIESGOS

SISTEMA INTEGRAL DE GESTIÓN
VICERRECTORÍA ADMINISTRATIVA Y FINANCIERA
UNIVERSIDAD TECNOLÓGICA DE PEREIRA

Contenido

TABLA DE FIGURAS

1. OBJETIVO

Establecer la metodología que permitan identificar, analizar, valorar y manejar eventos que puedan interferir con el logro de los objetivos y resultados institucionales

2. ALCANCE

Este procedimiento aplica a todos los procesos, OEC y facultades de la Universidad Tecnológica de Pereira y usuarios que requieran el uso de la metodología de gestión de riesgos

3. RESPONSABILIDADES

RESPONSABLE	RESPONSABILIDADES
Equipo para la Gestión de Riesgos	Proponer actualización de las directrices de gestión de riesgos y metodología para la administración de riesgos. Socializar la gestión de riesgos.
Usuarios de la metodología	Aplicar las directrices y la metodología establecida en el Manual de Gestión de Riesgos, por la UTP. Realizar actualización y seguimiento a al mapa de riesgos que corresponda, según su competencia, así: ● Líderes de los procesos ● Jefe de Planeación ● Grupo Técnico de Seguridad y Salud en el Trabajo ● Grupo Técnico de Seguridad de la Información ● Comité Centro de Laboratorios ● Director de Organismo Certificador. ● Facultades
Auditores internos de calidad	Auditar teniendo presente los lineamientos de la metodología para la administración riesgos establecida en la Universidad.
Control Interno	Realizar evaluación independiente a la gestión de riesgos en la Universidad.
Sistema Integral de Calidad	Actualización de la metodología y directrices, cuando sea pertinente.

4. ABREVIATURAS / DEFINICIONES

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 acontecimientos externos*

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.

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.

Nota*: Tratándose de riesgo fiscal, el impacto siempre será económico y se identificará en la redacción de riesgos como efecto dañoso, sobre bienes públicos, recursos públicos o intereses patrimoniales públicos*.

Causa Inmediata: Circunstancias bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo.

Nota*: Tratándose de riesgo fiscal, se usa el término circunstancia inmediata (Causa Inmediata, pero se asocia a la misma causa inmediata*.

Causa Raíz: Causa principal o básica, corresponde a las razones por la cuales se puede presentar el riesgo.

Nota*: También denominada Causa Eficiente o Causa Adecuada: Es el evento (acción u omisión) que de presentarse es generador directo de un efecto dañoso sobre los bienes, recursos o intereses patrimoniales de naturaleza pública. Es la condición necesaria, de tal forma que, si ese hecho no se produce, el daño no se genera. Así las cosas, la causa raíz se asocia con aquel hecho potencial generador del daño.*

Impacto: las consecuencias (afectación económica (o presupuestal) y/o afectación reputacional) que puede ocasionar a la organización la materialización del riesgo.

Riesgo Inherente: Nivel de riesgo propio de la actividad. El resultado de combinar la probabilidad con el impacto, nos permite determinar el nivel del riesgo inherente, dentro de unas escalas de severidad.

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

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).

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.

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

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.

Punto de Riesgo: Actividades en las que potencialmente se genera riesgo. Tratándose de riesgo fiscal los puntos de riesgo son todas las actividades que representen gestión fiscal, por ejemplo, aquellas de administración, gestión, ordenación, ejecución, manejo, adquisición, planeación, conservación, custodia, explotación, enajenación, consumo, adjudicación, gasto, inversión y disposición de los bienes o recursos públicos o intereses de naturaleza pública.

***Nota**: Para la identificación y priorización de los puntos de riesgo, la entidad deberá tener en cuenta aquellas actividades en las cuales se han presentado advertencias, alertas, hallazgos fiscales y/o fallos con responsabilidad fiscal, así como, aquellas actividades que la organización identifique que pueden generar riesgos fiscales. Para facilitar el ejercicio de identificación de puntos de riesgo consulte el Anexo: Catálogo Indicativo y Enunciativo de Puntos de riesgo fiscal y Circunstancias Inmediatas.*

Gestión de riesgo: Es el proceso que comprende el establecimiento y aplicación de las directrices, procedimientos, metodología e instrumentos que permiten brindar una seguridad razonable para controlar y responder a los acontecimientos potenciales, que puedan afectar los objetivos y resultados institucionales, contempla 4 etapas:

- **Identificación de riesgo:** Es la primera etapa que posibilita conocer los acontecimientos potenciales, que ponen en riesgo el alcance de los objetivos y los resultados institucionales y de procesos. La identificación comprende el establecimiento de los factores internos y externos que comprenden el contexto y la caracterización del riesgo.

- **Análisis de riesgo:** Es la segunda etapa, que permite establecer la probabilidad de ocurrencia de los acontecimientos que impacten el alcance de los objetivos, los resultados de la Institución y sus consecuencias.
- **Valoración de riesgo:** Es la tercera etapa, donde se determina la priorización de los riesgos en relación con los controles establecidos.
- **Manejo de riesgo:** Es la cuarta etapa, donde permite establecer el tratamiento a seguir para mitigar o prevenir los riesgos de acuerdo al nivel de exposición. Contempla la implementación de acciones preventivas.
- **Acciones preventivas:** se anticipan a la causa, y pretenden eliminarla antes de su existencia. Evitan los problemas identificando los riesgos. Cualquier acción que disminuya un riesgo es una acción preventiva.
- **Tratamiento del Riesgo:** establece los tratamientos que deberán ser realizados para evitar, reducir, transferir compartir y asumir para disminuir el nivel de exposición.
- **Plan de Mitigación:** corresponde a los planes de contingencia que se hayan formulado previamente o actividades que el proceso ha establecido con anterioridad

Control del riesgo: Es toda acción que tiende a prevenir o mitigar los riesgos, significa analizar el desempeño de los procesos, evidenciando posibles desviaciones frente al resultado esperado. Los controles proporcionan un modelo operacional de seguridad razonable en el logro de los objetivos.

Aplicación del control Emplear o poner en práctica un control con el propósito de que no se materialice el riesgo. No implica que el control sea efectivo para la prevención o mitigación del riesgo

Aspectos ambientales: Entorno en el cual opera la Universidad, incluyendo el aire, agua, suelo, recursos naturales, flora, fauna, seres humanos y sus interrelaciones.

Impactos ambientales: Cualquier cambio en el medio ambiente ya sea adverso o beneficioso, como resultado total o parcial de los aspectos ambientales de la Universidad.

Efectividad del control: Se refiere a que la aplicación del control puede dar como resultado la prevención o mitigación del riesgo

Usuarios de la metodología: Se refiere a los procesos del sistema integral de gestión, facultades, plan de desarrollo institucional, sistema de seguridad y salud en el trabajo, sistema de seguridad de la información, laboratorios de ensayo y calibración y organismo certificador.

Sistema de Gestión de Riesgos para la Integridad Pública -SIGRIP: esquema que define la interrelación e interacción de diferentes elementos para asegurar una gestión integral de los riesgos que afectan la integridad pública. El SIGRIP se articula con la Política para la Gestión Integral de Riesgos.

Riesgos para la integridad: Toda actuación o decisión de las y los servidores públicos, así como de otros colaboradores de las entidades públicas que privilegien el interés particular sobre el general, asociadas a conductas no deseadas que van en contravía de los valores del servicio público. Incluido, también, el riesgo de que la integridad de la entidad sea utilizada para dar apariencia de legalidad a los activos provenientes de actividades delictivas o para canalizar recursos hacia la realización de actividades terroristas

Soborno: ofrecer, prometer, dar, aceptar o solicitar una ventaja indebida de cualquier valor (que puede ser financiero o no financiero), directa o indirectamente, e independientemente de la ubicación, en violación de la ley aplicable, como incentivo o recompensa para que una persona actúe o se abstenga de actuar. (A partir de ISO37001:2025)

Soborno entrante: ofrecer, prometer, dar, aceptar o solicitar una ventaja indebida a un servidor de la entidad.

Soborno saliente: ofrecer, prometer, dar, aceptar o solicitar una ventaja indebida por parte de servidores públicos a otros en nombre de la entidad.

Fraude: errores, omisiones, informes inexactos o descripciones incorrectas realizados con culpa o dolo para beneficio personal o de terceros. Puede ser interno, en cuyo caso el fraude involucra a colaboradores, o externo, cuando se realiza por terceros, externos y la organización es la víctima. (A partir de ISO37001:2025)

Conflicto de interés: Se presenta cuando el interés general, propio de la función pública, entre en conflicto con un interés particular y directo del servidor público. El interés del servidor público se presenta cuando debe decidir sobre asuntos en los que tiene un interés particular y directo en su regulación, gestión, control o decisión, o lo tiene su cónyuge, compañero o compañera permanente, o algunos de sus parientes dentro del cuarto grado de consanguinidad, segundo de afinidad o primero civil, o su socio o socios de hecho o de derecho. (A partir de la Ley 1952 de 2019, art. 44, Ley 734 de 2002 y algunas disposiciones de la Ley 1474 de 2011)

Corrupción: Todo acto que implique desviación de la gestión administrativa o de los recursos públicos y privados para obtener un beneficio propio o para un tercero. Igualmente, constituyen actos de corrupción las conductas punibles descritas en la Ley 599 de 2000, o en cualquier ley que la modifique, sustituya o adicione, así como lo previsto en la Ley 1474 de 2011; las faltas disciplinarias; y las conductas generadoras de responsabilidad fiscal relacionadas con los actos de corrupción y cualquier comportamiento contemplado en las convenciones o tratados contra la corrupción que Colombia haya suscrito y ratificado. Esas conductas incluyen: (i) El uso del poder para obtener

Lavado de activos: el artículo 323 de la Ley 599 de 2000, define el delito de lavado de activos como la conducta desplegada por quien "adquiera, resguarde, invierta, transporte, transforme, almacene, conserve, custodie o administre bienes que tengan su origen mediato o inmediato en actividades [relacionadas con un delito fuente], o vinculados con el producto de delitos ejecutados bajo concierto para delinquir, o les dé a los bienes provenientes de dichas actividades apariencia de legalidad o los legalice, oculte o encubra la verdadera naturaleza, origen, ubicación, destino, movimiento o derecho sobre tales bienes o realice cualquier otro acto para ocultar o encubrir su origen ilícito". El Lavado de Activos puede darse por: colocación, ocultamiento e integración.

Delito fuente: según el artículo 323 de la Ley 599 de 2000, son delitos fuente del lavado de activos: tráfico de migrantes, trata de personas, extorsión, enriquecimiento ilícito, secuestro extorsivo, rebelión, tráfico de armas, tráfico de menores de edad, financiación del terrorismo y administración de recursos relacionados con actividades terroristas, tráfico de drogas tóxicas, estupefacientes o sustancias sicotrópicas, delitos contra el sistema financiero, delitos contra la administración pública, contrabando, contrabando de hidrocarburos o sus derivados, fraude aduanero o favorecimiento y facilitación del contrabando, favorecimiento de contrabando de hidrocarburos o sus derivados, en cualquiera de sus formas.

Colocación: es la disposición del dinero proveniente de actividades delictivas. Durante esta fase inicial, el determinador o autor introduce sus fondos ilegales en actividades legales o aparentemente legales, bien a través del sistema financiero o de otros tipos de negocios o contratos, tanto nacionales como internacionales.

Ocultamiento: es la separación de fondos ilícitos de su fuente mediante una serie de transacciones, cuyo fin es desdibujar la transacción ilícita original. Esta etapa supone la conversión de los fondos procedentes de actividades ilícitas a otra forma y crear esquemas complejos de transacciones financieras para disimular el rastro documentado, la fuente y la propiedad de los fondos.

Integración: es dar apariencia legítima a riqueza ilícita mediante el reingreso en la economía con transacciones comerciales o personales que aparentan ser normales. Esta fase conlleva lacolocación de los fondos lavados de vuelta en la economía para crear una percepción de legitimidad. El lavador

podría optar por invertir los fondos en bienes raíces, artículos de lujo o proyectos comerciales, entre otros.

Financiación del Terrorismo (FP): el artículo 345 de la Ley 599 de 2000, define el delito de lavado de activos como la conducta desplegada por quien "directa o indirectamente provea, recolecte, entregue, reciba, administre, aporte, custodie o guarde fondos, bienes o recursos, o realice cualquier otro acto que promueva, organice, apoye, mantenga, financie o sostenga económicamente a grupos de delincuencia organizada, grupos armados al margen de la ley o a sus integrantes, o a grupos terroristas nacionales o extranjeros, o a terroristas nacionales o extranjeros, o a actividades terroristas". La Financiación del Terrorismo puede darse por: recaudación, transmisión, utilización.

Recaudación: consiste en la búsqueda de fuentes de financiación por las organizaciones terroristas, bien sean de origen legal, como los aportes de los Estados, individuos, entidades, organizaciones y donantes en general que apoyan su causa o son engañados, así como recursos provenientes de cualquier actividad delictiva, fondos que generalmente circulan en efectivo.

Transmisión: es la fase intermedia que busca poner el dinero recaudado a disposición de la organización terrorista, quedando simplemente la espera de su utilización final; corresponde al movimiento de los fondos a través de distintas técnicas, se trata de ocultar sus movimientos y destino final.

Utilización: fase donde los fondos se utilizan básicamente para la financiación de la logística estructural de la organización o la logística operativa en materia de planeación y ejecución de actos terroristas.

Financiación de la Proliferación de Armas de Destrucción Masiva (FP): fondos u otros activos a disposición, directa o indirectamente, de o para el beneficio de, alguna persona o entidad designada por o bajo la autoridad del Consejo de Seguridad de las Naciones Unidas dentro del Capítulo VII de la Carta de las Naciones Unidas, en lo relativo a la prevención, represión e interrupción de la proliferación de armas de destrucción masiva y su financiamiento. La Financiación de la Proliferación puede darse por: recaudación, transmisión, utilización

Debida diligencia (due dilligence): proceso que deben llevar a cabo las entidades para identificar, prevenir, mitigar y explicar cómo abordan los impactos negativos reales y potenciales en sus propias actividades, su cadena de suministro y otras relaciones comerciales.

Debida diligencia en el conocimiento de la contraparte (debida diligencia del cliente): proceso que le permite a la entidad conocer aspectos relevantes de sus contrapartes, sean partes vinculadas o

relacionadas, para poder gestionar el riesgo que cualquier vinculación o relacionamiento genera.

Función de cumplimiento: función que debe distribuirse dentro de la organización que asigna a una persona, grupo o dependencia la responsabilidad de adoptar medidas para promover el cumplimiento interno, administrar los riesgos para la integridad pública de conformidad con las políticas institucionales de gestión de riesgos, apoyar los procesos de evaluación de los Sistemas de Gestión del Riesgo, realizar un control de segunda línea y asesorar a la Alta Dirección en el direccionamiento estratégico de la organización desde un enfoque basado en riesgos para proteger la integridad pública.

Contraparte: cualquier persona o entidad que tenga un interés propio o particular, diferente al interés de la organización.

Parte Interesada: es un tipo de contraparte con la cual no se ha establecido ninguna relación o vinculo, pero que ha manifestado formalmente su interés en establecerlo.

Parte Vinculada: para efectos del SIGRIP, es una contraparte dependiente de la organización con la cual se ha establecido una relación de especial de sujeción por su relación legal o reglamentaria, o laboral.

Parte Relacionada: para efectos del SIGRIP, es una contraparte independiente de la organización con la cual se ha establecido una relación comercial, contractual o legal; o respecto de la cual se ejerce algún grado de control jerárquico, de tutela o de propiedad, sin detrimento de su independencia. Teniendo en cuenta el Anexo Técnico que establece la articulación en la Gestión Integral del Riesgo para Entidades Públicas pertenecientes al Sistema de Seguridad Social en Salud, a continuación, se precisan los conceptos específicos aplicables para las entidades de este sector

Subsistema de Administración del Riesgo de Corrupción, Opacidad y Fraude – SICOF: Conjunto de políticas, principios, normas, procedimientos y mecanismos de verificación y evaluación establecidos por el máximo órgano social u órgano equivalente, la alta dirección y demás funcionarios de una organización para proporcionar un grado de seguridad razonable en cuanto a la consecución de los siguientes objetivos:

- Mejorar la eficiencia y eficacia en las operaciones de las entidades sometidas a inspección y vigilancia evitando situaciones de Corrupción, Opacidad y Fraude. Para el efecto, se entiende por eficacia la capacidad de alcanzar las metas y/o resultados propuestos; y por eficiencia la capacidad de producir el máximo de resultados con el mínimo de recursos, energía y tiempo.
- Prevenir y mitigar la ocurrencia de actos de Corrupción, Opacidad y Fraudes, originados tanto

al interior como al exterior de las organizaciones.

- ✓ Realizar una gestión adecuada de los Riesgos

Sistema de Control Interno: sistema integrado por el esquema de organización y el conjunto de los planes, métodos, principios, normas, procedimientos y mecanismos de verificación y evaluación adoptados por una entidad, con el fin de procurar que todas las actividades, operaciones y actuaciones, así como la administración de la información y los recursos, se realicen de acuerdo con las normas constitucionales y legales vigentes dentro de las políticas trazadas por la dirección y en atención a las metas u objetivos previstos.

5. FORMATOS O IMPRESOS

- Directrices para la gestión de riesgos
- Formato Mapa de riesgos (1313-SIG-F13).

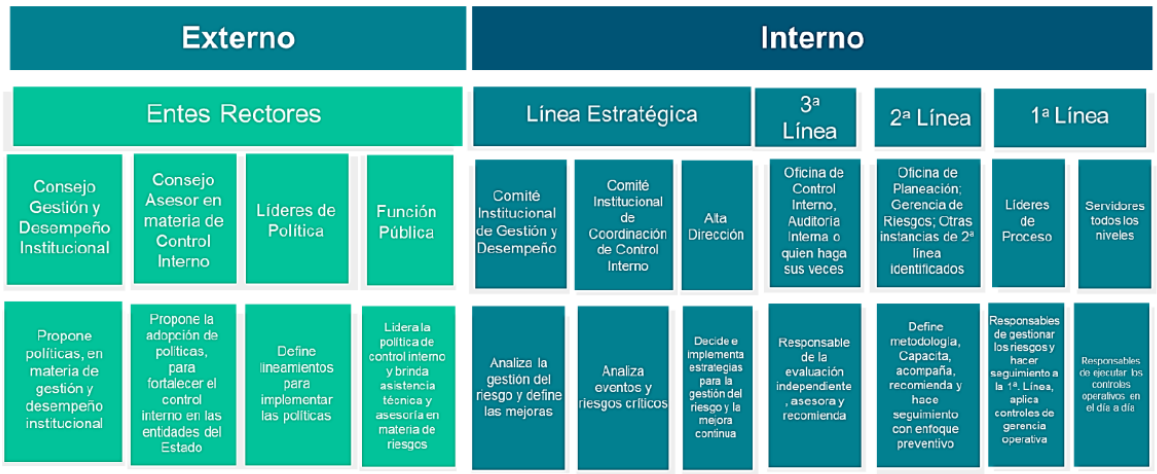
6. GESTIÓN DE RIESGOS

La gestión de riesgos en la Universidad Tecnológica de Pereira, se realizará de acuerdo a las directrices para la gestión de riesgos y los procedimientos establecidos en este Manual, los cuales se basan en documentos internos y externos, de tipo legal o reglamentario en Gestión de Riesgos, en particular, se encuentra muy alineado a la "Guía para la Gestión Integral del Riesgo en Entidades Públicas", versión 7.

6.1 REVISIÓN Y APLICACIÓN DE LA METODOLOGÍA

Los roles y responsabilidades frente a la gestión de riesgos, se encuentran establecidos en las DIRECTRICES, tomando como criterio principal, lo definido en dicha materia por la Función pública.

Figura 1. Institucionalidad de MIPG desde la perspectiva de Gestión del riesgo.



Fuente: Dirección de Gestión y Desempeño Institucional de Función Pública, 2025.

Nota: En entidades de alta complejidad se puede considerar la figura de gestores de riesgos. Se trata de personas clave en las áreas o procesos que ayudan al líder de proceso y a la 2ª línea de defensa en la gestión del riesgo, esta figura es opcional no obligatoria en su implementación.

Fuente: Función Pública

6.1.1 REVISIÓN

Revisar y proponer actualización sobre las directrices y el procedimiento para la gestión de riesgos. Así mismo, presentar propuesta de mejora acerca de la metodología e instrumentos utilizados en la gestión de riesgos al Comité Institucional de Control Interno

6.1.2 ASESORÍA Y DIFUSIÓN

El equipo para la gestión de riesgos es el encargado de asesorar en la implementación y aplicación de las directrices y metodología a los usuarios (dependencias académicas y administrativas de la UTP).

El Sistema Integral de Gestión será el responsable de asegurar la correcta publicación de documentos asociados a la Gestión de Riesgos, y divulgar a todos los usuarios, la información correspondiente a las directrices y metodología.

6.2 INTRODUCCIÓN A LA MATRIZ DE RIESGOS

La gestión de riesgos en la Universidad contempla la formulación de un mapa de riesgos, el cual se encuentra integrado dentro del formato 1313-SIG-F13, se compone de las siguientes hojas:

- Hoja 1. Matriz de Riesgos – Identificación del riesgo

- Hoja 2. Matriz de Riesgos – Valoración del riesgo
- Hoja 3. Matriz de Riesgos – 1er. Seguimiento a riesgos: se realiza, con el fin de realizar seguimiento y medición a la gestión de riesgos del primer semestre de cada anualidad, se realiza seguimiento a: indicador del riesgo con análisis, análisis de los controles existentes, cumplimiento y análisis de las acciones de manejo planteadas, análisis de la eficacia de dichas acciones y la situación del riesgo después del seguimiento
- Hoja 4. Matriz de Riesgos – 2do. Seguimiento a riesgos; se realiza, con el fin de realizar seguimiento y medición a la gestión de riesgos del segundo semestre de cada anualidad, se realiza seguimiento a: indicador del riesgo con análisis, análisis de los controles existentes, cumplimiento y análisis de las acciones de manejo planteadas, análisis de la eficacia de dichas acciones y la situación del riesgo después del seguimiento

Las matrices se elaboran, administran y visualizan, de acuerdo al TIPO DE MAPA, así:

- **Proceso** *(Todas las dependencias administrativas y académicas)*
- **PDI (***Unidades organizacionales asociadas a los pilares del PDI)*
- **OEC** *(Todos los Organismos Evaluadores de la conformidad (Laboratorios Acreditados)*

6.3 ETAPAS PARA LA CONSTRUCCIÓN DEL MAPA GENERAL DE GESTIÓN DE RIESGOS

6.3.1 IDENTIFICACIÓN DEL RIESGO (Hoja 1 – Matriz de Riesgos)

- Una vez se selecciona el TIPO DE MAPA, este se articula las áreas de impacto que corresponden a cada TIPO.
- **Áreas de impacto:** se identifica la dependencia (administrativa o académica) responsable de la gestión del riesgo, así como, su líder desde dicha dependencia, objetivo del proceso / PDI / OEC. 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
- **Mapa institucional**: esta identificación, se selecciona “SI”, solo para riesgos de corrupción y riesgos estratégicos. Desde el equipo de riesgos, se identificarán aquellas otras, que, de acuerdo a su criterio, tiendo como principal factor decisorio el nivel de impacto que genera a nivel institucional.
- **Factor de Riesgo**: son las fuentes generadoras de riesgos, es decir, circunstancias o condiciones que aumenta la probabilidad de que ocurra el evento de riesgo, bien sea de fuente interna o externa. No son causas directas, pero incrementan el nivel de exposición.

En la figura 1. se establece un listado con los factores de riesgo que pueden incidir en un proceso, los cuales podrán ampliarse o adecuarse de acuerdo con las características propias de cada proceso o entidad, sector donde se desenvuelve y otros aspectos que puedan determinar factores adicionales que deban ser contemplados para una adecuada identificación del riesgo. Esta tabla incluye los factores incluidos en todos los tipos de riesgos: generales, fiscales, de seguridad de la información y para la integridad pública (SIGRIP).

Figura 2. Factores de Riesgo / Fuentes Generadoras del evento

Factor	Definición		Fuentes generadora de evento
Ejecución y administración de procesos	Eventos relacionados con la ejecución de los procesos y procedimientos determinados para la operación de la entidad, uso de sistemas de información, por errores en las actividades que deben realizar los servidores de la organización. Estructura organizacional que afecta la capacidad organizacional		Falta de aplicación de los procedimientos
			Falta segregación de funciones
			Errores de grabación, autorización
			Falta de super visión o interventoría
			Errores en cálculos para pagos internos y externos
			Alta rotación o insuficiencia de personal
			Acciones contrarias a las leyes o acuerdos de empleo, salud o seguridad en el trabajo
			Acciones contrarias a las leyes o acuerdos contractuales
			Falta de capacitación y otros temas relacionados con el personal
Transacción u Operación (aplica para LA/FT/FP	Eventos relacionados con transacciones y Operaciones realizadas por un cliente o usuario, que accede o entrega un bien o servicio a la entidad, a través de los canales dispuestos y en una jurisdicción específica.		Contrapartes de la entidad (naturales o jurídicas)
			Productos (bienes o servicios) que oferta/requiere
			Canales utilizados para la operación
			Jurisdicciones (nacional o territorial)
Talento humano	Eventos relacionados con las conductas o comportamientos de los empleados que afectan la Integridad Pública		Fraude Interno
			Soborno
			Gestión inadecuada de conflicto de Intereses
			Corrupción
			Hurto activos

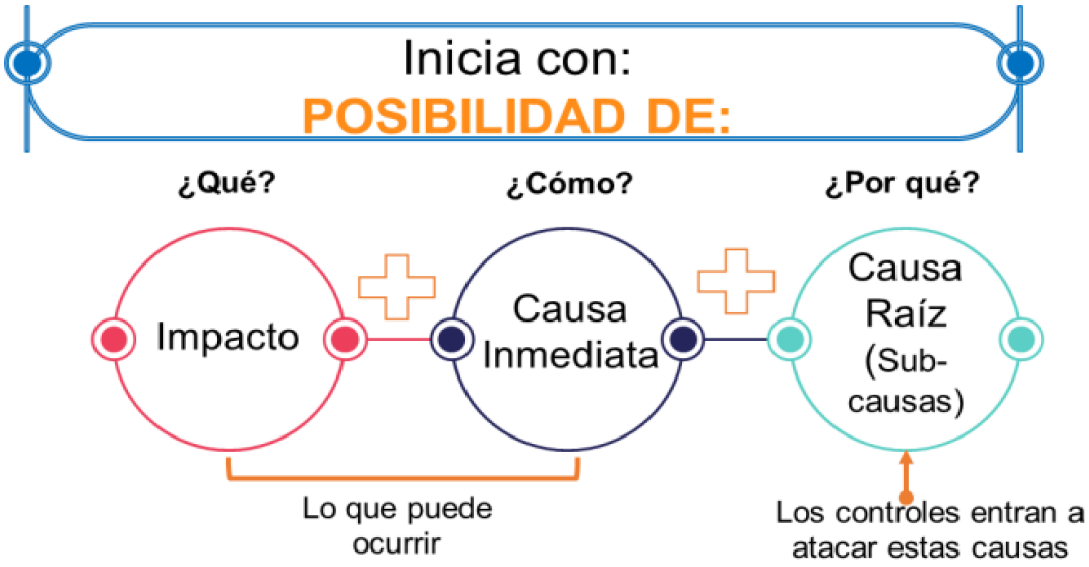
Factor	Definición		Fuentes generadora de evento
Tecnología	Eventos relacionados con la infraestructura tecnológica de la entidad		Daño de equipos
			Caída de sistemas de información y aplicaciones
			Caída de redes
			Errores en hardware o software
			Errores en programas
Infraestructura	Eventos relacionados con la infraestructura física de la entidad.		Derrumbes
			Incendios
			Inundaciones
			Daños a activos fijos
Evento externo	Eventos por situaciones externas que afectan la entidad		Fraude Externo
			Suplantación de identidad
			Asalto a la oficina
			Atentados, vandalismo, orden público

***Fuente**: Guía para la Gestión Integral de Riesgos en Entidad Públicas.*

- **Tipología**: se selecciona la categoría a la que pertenece el riesgo en proceso de identificación, siendo las opciones:
  - **Gestión**: riesgos asociados a fallas en la planeación, ejecución, control o toma de decisiones que pueden afectar el cumplimiento de objetivos institucionales.
  - **Fiscal**: Riesgos relacionados con el uso inadecuado, pérdida o detrimento de los recursos públicos, con impacto patrimonial para la institución o el Estado.
  - **Seguridad de la Información**: Riesgos que comprometen la confidencialidad, integridad o disponibilidad de la información y de los sistemas que la soportan.
  - **Integridad pública – corrupción**: Riesgos vinculados a conductas indebidas como soborno, fraude, conflicto de intereses o abuso de poder que afectan la ética y la transparencia institucional.
  - **Integridad pública – LA / FT / FP**: Riesgos asociados al Lavado de Activos, la Financiación del Terrorismo y la Financiación de la Proliferación de armas de destrucción masiva, que pueden comprometer la legalidad y reputación de la entidad.

- **Descripción del tipo del riesgo**: Impacto + Causa Inmediata + Causa Raíz. Con el fin de facilitar la redacción adecuada del riesgo y desplegar todos los detalles necesarios para la identificación, se propone la estructura que se muestra en la figura 2.

Figura 3. Estructura para la redacción del riesgo



***Fuente**: Guía para la Gestión Integral de Riesgos en Entidades Públicas.*

- **IMPACTO**: *son las consecuencias (afectación económica o presupuestal) y/o afectación reputacional que puede ocasionar a la organización la materialización del riesgo. Este se categoriza en tres opciones dentro de la matriz de gestión de riesgos:*
  - *Posibilidad de pérdida económica*
  - *Posibilidad de pérdida reputacional*
  - *Posibilidad de pérdida económica y reputacional*
- **CAUSA INMEDIATA**: *son las 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.*

  Estos dos elementos permiten plantear el evento no deseado (¿qué puede ocurrir?), es decir la situación, acción, condición o suceso incierto que, si ocurre, podría afectar el logro de los objetivos de la entidad.

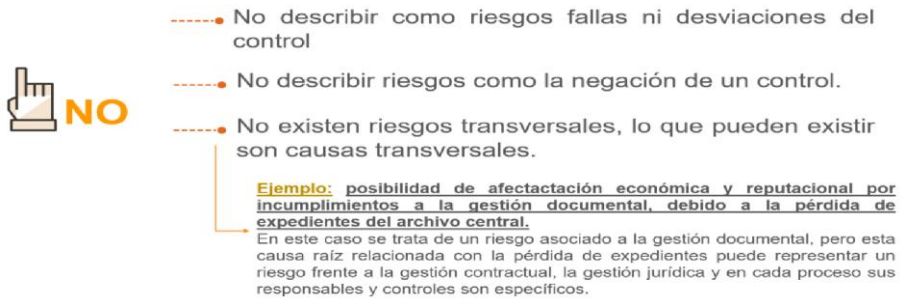
  Características clave: Debe ser específico y claro, no genérico. Expresado en términos de qué podría pasar.

- **CAUSA RAÍZ**: *Se plantea ¿por qué puede ocurrir? el evento no deseado, bajo el análisis de la causa principal o básica, corresponden a las razones por la cuales se puede presentar el riesgo, información esencial para la definición de controles en el paso 3 de diseño y análisis de controles. Se debe tener en cuenta que para un mismo riesgo pueden existir más de una causa o subcausas que pueden ser analizadas.*

  Las características clave: Identificar causas raíz y condiciones contribuyentes que pueden clasificarse en: humanas, tecnológicas, normativas, ambientales, organizacionales. Un adecuado análisis de causa raíz debe permitir diferenciar la causa raíz, de la causa inmediata, entendida esta última como las circunstancias más evidentes sobre las cuales se presenta el riesgo y que en ocasiones, no constituyen la causa principal del riesgo.

  Se recomienda para una adecuada redacción del riesgo, tener en cuenta algunas premisas como las que se muestran en la figura 3.

Figura 4. Premisas para una adecuada redacción del riesgo.



***Fuente**: Guía para la Gestión Integral de Riesgos en Entidad Públicas.*

Bajo las anteriores consideraciones, una representación simplificada del modelo de descripción del riesgo contiene los siguientes elementos:

- *Evento no deseado y sus posibles consecuencias: ¿Qué puede pasar?*
- *Causas: ¿Por qué puede pasar?*
- *Tipología: ¿A qué categoría pertenece?*
- *Factor de riesgo: ¿Qué condición aumenta su probabilidad?*

Características del riesgo:

- No se puede evitar (siempre existe).
- Los controles se establecen sobre las causas que lo generan, no sobre los mismos riesgos.

6.3.2 ANÁLISIS DEL RIESGO INHERENTE (Hoja 1 – Matriz de Riesgos)

Los riesgos identificados se analizan de acuerdo a su probabilidad e impacto.

- **Probabilidad:** posibilidad de ocurrencia del riesgo, 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.***

Figura 5. Criterios para definir el nivel de probabilidad.

PROBABILIDAD				
ALTA 100%	**MEDIA ALTA 80%**	**MEDIA 60%**	**MEDIA BAJA 40%**	**BAJA 20%**
La actividad que conlleva el riesgo se ejecuta más de **5000 veces por año**	La actividad que conlleva el riesgo se ejecuta más de **500 veces al año y máximo 5000 veces por año**	La actividad que conlleva el riesgo se ejecuta de **25 a 500 veces por año**	La actividad que conlleva el riesgo se ejecuta de **3 a 24 veces por año**	La actividad que conlleva el riesgo se ejecuta como **máximos 2 veces por año**

***Fuente**: Propia.*

- **Impacto:** son las consecuencias que puede ocasionar a la entidad por la materialización de un riesgo. Se definen dos criterios fundamentales, en los cuales se agrupan todos los criterios conocidos en versiones anteriores de la metodología de gestión de riesgos, estos criterios son: Impactos económicos y reputacionales.

  Cuando se presenten ambos impactos para un riesgo, apéndice 6.3.1 descripción del tipo de riesgo - "*Impacto*", se deberá seleccionar tanto económico como reputacional con diferentes niveles, se deberá tomar el nivel más alto

  Por ejemplo:

  - Riesgo identificado con impacto económico en nivel MEDIO
  - Impacto reputacional en nivel MEDIO ALTO

  Entonces, se tomará el más alto, en este caso sería el nivel MEDIO ALTO.

En la figura 5, se establecen los criterios para definir el nivel de impacto.

Figura 6. Criterios para definir el nivel de impacto.

	IMPACTO				
	ALTO	**MEDIO-ALTO**	**MEDIO**	**MEDIO-BAJO**	**BAJO**
AFECTACIÓN REPUTACIONAL	El riesgo afecta la imagen de la entidad a **nivel nacional**, con efecto publicitario sostenido a nivel país	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a **nivel de sector educación, nivel departamental o municipa**l	El riesgo afecta la imagen de la entidad con **algunos usuarios de relevancia** frente al logro de los objetivos.	El riesgo afecta la imagen de la entidad a nivel interno, de conocimiento general, del **comité directivo y/o consejo superior.**	El riesgo afecta la imagen de algún **área de la entidad.**
AFECTACIÓN ECONÓMICA	Mayor a 500 SMLMV	Mayor a 100 SMLMV y Menor a 500 SMLMV	Mayor a 50 SMLMV y Menor a 100 SMLMV	Mayor a 10 SMLMV y Menor a 50 SMLMV	Afectación menor a 10 SMLMV

Fuente: Propia

- **Prioridad Inicial** (Riesgo Inherente): se obtiene la calificación del riesgo inherente, para ello, se deberá individualizar la escala de calificación de la probabilidad y el impacto para cada uno de los riesgos; al finalizar el análisis, se cruzan las dos variables (*probabilidad / Impacto*), obteniendo el mapa de calor, de los riesgos inherentes, que, como se observa en la figura 6, conta de 3 zonas de calor (**LEVE**, **MODERADO**, **GRAVE**).

Figura 7. Mapa de calor – Riesgo Inherente

	CA SI SEGURO	**ALTA**	**5**	5	10	15	20	25
	P ROB A B LE	**MEDIA-ALTA**	**4**	4	8	12	16	20
	P OSIB LE	**MEDIA**	**3**	3	6	9	12	15
	IM P ROB A B LE	**MEDIA-BAJA**	**2**	2	4	6	8	10
	RA RO	**BAJA**	**1**	1	2	3	4	5
				1	**2**	**3**	4	**5**
				BAJO	**MEDIO-BAJO**	**MEDIO**	**MEDIO-ALTO**	**ALTO**
				INSIGNIFICANTE	**MENOR**	**MODERADO**	**MAYOR**	**CATASTROFICO**
				IMPACTO				

Fuente: Propia.

6.3.3 VALORACIÓN DEL RIESGO - (Hoja 2 – Matriz de Riesgos)

- **DISEÑO DE CONTROLES**

Los riesgos se valoran de acuerdo a los controles existentes, los cuales se pueden clasificar tres categorías, ver figura 7.

Figura 8. Características de los controles

TIPO DE CONTROL	DESCRIPCIÓN	ACCIONADO	IDEAL, CUANDO SE BUSCA
PREVENTIVO	Condiciones que aseguran el resultado final esperado, con la aplicación del control.	En la entrada del proceso	Evitar / Reducir riesgo
DETECTIVO	Detectan el riesgo, generalmente ocasionan reprocesos.	Durante la interacción de las actividades del proceso	Mitigar / Reducir el riesgo. Complementa con controles correctivos.
CORRECTIVO	Se implementan de forma preventiva, sin embargo, requieren una serie de acciones que garanticen que se puedan usar en el momento en que se materialice un riesgo.	En la salida del proceso.	Mitigar / Reducir el impacto, después de la materialización de un riesgo. Tienen un costo implícito.

Fuente: Propia

En esta etapa se realiza el diseño y evaluación de los controles, calificándolos de acuerdo a la situación en la cual estos se encuentren, se compone de los siguientes campos:

- **Estado del control:** se selecciona la opción más apropiada, de acuerdo al estado actual del control, tomando como base la existencia o inexistencia del mismo.
    - **No Existen**: No existen controles asociados al riesgo para su prevención o mitigación.
    - **Regularmente confiables**: Los controles existentes, son aplicados, pero no existe certera de su efectividad para la prevención o mitigación del riesgo.
    - **Confiables No aplicados**: Los controles existentes no son aplicados por el responsable para la prevención o mitigación del riesgo.
    - **Aplicados, Confiables y No documentados:** Los controles existentes aplicados y que son efectivos para la prevención o mitigación del riesgo no se encuentran documentados.

- **Aplicados, Confiables y Documentados**: Los controles existentes son aplicados, efectivos para la prevención o mitigación del riesgo y se encuentran documentados.

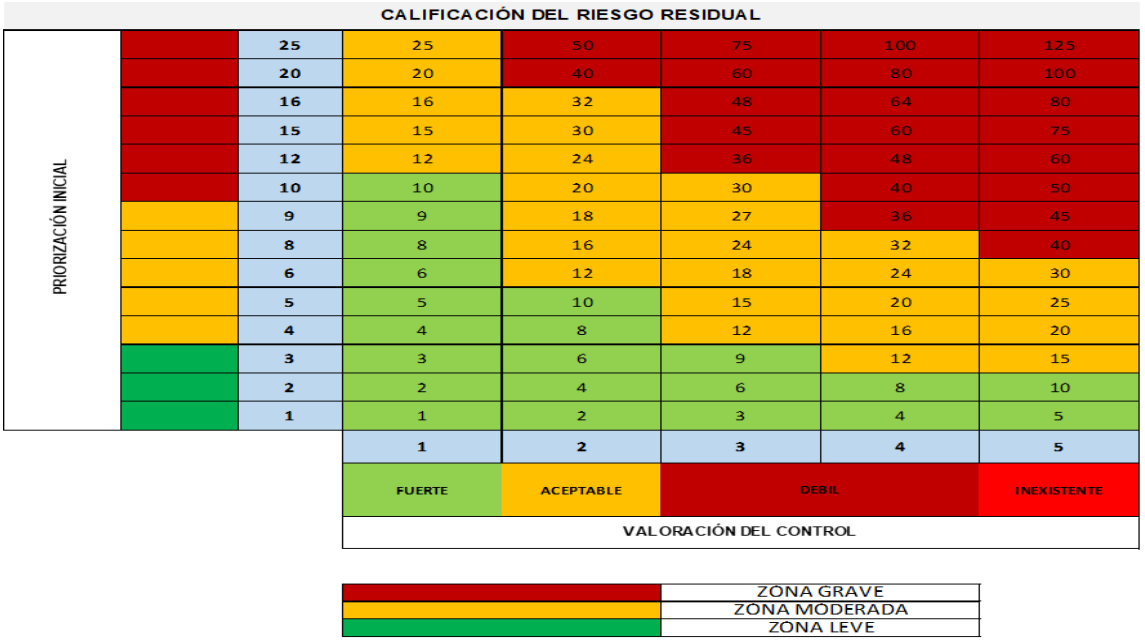
- **Descripción del Control (Acción):** Determina para qué se realiza el control, se utilizar verbos fuertes como: Verificar, validar, conciliar, comparar, revisar, cotejar, detectar.
- **Nivel de automatización:** refiere el grado de automatización del control, todo control que requiera el registro o ejecución de una persona en pequeña o gran medida, se entiende que es "Manual". Siendo "Automático" cuando el control se ejecuta automáticamente por cualquier máquina, sin intervención humana.
- **Nombre del Aplicativo / software**: solo, cuando el nivel de automatización es "Automático", se deberá referenciar el nombre del instrumento objeto de la automatización.
- **Asignación de Responsabilidad**: determina, sí el control ha sido asignado o no a un responsable dentro de la institución.
- **Responsable**: determina el cargo del responsable que ejecuta el control, se deberá considerar la estructura organizacional y las diferentes denominaciones de empleos (directivos, asesores, profesionales, técnicos, asistenciales), así como su despliegue en grupos de trabajo internos, equipos o comités. Cuando se trate de controles automáticos se identificará el responsable de su calibración o parametrización periódica en el sistema de información o software a través del cual opere el control.
- **Periodicidad de la aplicación**: define, si la aplicación de la frecuencia de aplicación del control es Oportuna o No.
- **Frecuencia de Aplicación**: corresponde a la periodicidad con la cual se ejecuta una actividad de control debe ser adecuada para detectar o prevenir el riesgo en función de su nivel de exposición inherente. (puede ser periódica o por evento).
- **Tipología del control**: Detectivo, Preventivo y Correctivo; con el fin de precisar cuándo se activa un control de acuerdo a su tipificación, se dan las denominaciones a continuación, ver figura 8:

Figura 9. Cadena de valor del proceso y tipologías de controles

***Fuente**: Guía para la Gestión Integral de Riesgos en Entidad Públicas.*

Para lograr la valoración de los riesgos, se cruza la evaluación del control con el resultado de la calificación de riesgo inherente en la matriz de riesgo residual, obteniéndose como resultado el nivel de exposición al riesgo así:

Figura 10. Mapa de calor del riesgo residual.



Fuente: propia

6.3.4 ANALISIS DEL RIESGO RESIDUAL (Hoja 2 – Matriz de Riesgos)

El análisis del riesgo residual, se realiza en razón a los resultados obtenidos en la matriz de calor del riesgo residual (Figura 9), de allí, se realiza la clasificación del riesgo, de acuerdo al nivel de exposición.

- **NIVEL DE EXPOSICIÓN AL RIESGO**: De acuerdo al resultado obtenido en la matriz de riesgo residual se define el nivel de exposición del riesgo (**GRAVE**, **MODERADO**, **LEVE**), con lo cual se determina el tratamiento para el riesgo.

Figura 11. Opciones de manejo de acuerdo al nivel de exposición al riesgo.

NIVEL DE EXPOSICIÓN AL RIESGO	OPCIÓN DE TRATAMIENTO	ACCIONES A TOMAR
GRAVE Riesgos con	Evitar Reducir	Se deberá implementar inmediatamente las acciones preventivas que conlleven a evitar, reducir, transferir o compartir el riesgo

NIVEL DE EXPOSICIÓN AL RIESGO	OPCIÓN DE TRATAMIENTO	ACCIONES A TOMAR
calificación superior o igual a 36	Transferir Compartir	Las acciones preventivas tomadas deberán conllevar a implementar nuevos controles que prevengan la materialización del riesgo y a mitigar el impacto.
MODERADO Riesgos con calificación entre 12 y 32	Reducir Transferir Compartir	Se deberá implementar acciones preventivas que conlleven a reducir, transferir o compartir el riesgo Se deberá implementar acciones preventivas que conlleven a mejorar el diseño o eficacia de los controles existentes.
LEVE Riesgos con calificación inferior o igual a 10	Asumir	Se debe realizar seguimiento a los riesgos con el fin de verificar su impacto, probabilidad y la valoración de los controles

Fuente: Propia.

- **INDICADOR DEL RIESGO:** Se debe formular un indicador que permita monitorear el comportamiento del riesgo respecto al tratamiento y las acciones emprendidas para su manejo, se plantea la formula y meta, con la cual se realizará seguimiento a la gestión del riesgo, y permitirá poder identificar la posible materialización del mismo.
    - Formula: se establece la formula, mediante la cual se realiza la medición.
    - Meta: se establece el limite inferior, superior o valor exacto, mediante el cual se medirá la efectividad del control, con relación a la aplicación de la formula que mide el indicador.

- **MANEJO DEL RIESGO:** Se deben formular acciones preventivas de acuerdo al tratamiento seleccionado para los riesgos que se encuentren en los niveles de exposición grave y moderado.
    - **Tipo**: se selecciona el tipo de acción de manejo a implementar, luego de controles; se clasifican en:

    - Evitar: Consiste en eliminar de forma definitiva la actividad que genera riesgo.
    - Reducir: Implica implementar controles que conlleven a disminuir la probabilidad de ocurrencia del riesgo o su nivel de impacto.
    - Transferir: Se refiere a implementación de controles para que un tercero externo a la Universidad asuma el riesgo, para lo cual se deberá contar con la autorización del Vicerrector Administrativo y Financiero.
    - Compartir: Consiste en establecer controles de manera conjunta con otro proceso al interior de la Universidad
    - Asumir: Se refiere a implementar acciones de seguimiento que conlleven al análisis del riesgo

- **Acción:** Son las acciones de manejo, posteriores a los controles, ayudan a evitar la materialización del riesgo luego de implementados los controles, es decir, sin embargo, de acuerdo al nivel de exposición al riesgo, no siempre se requiere establecer acciones de manejo, es decir, siempre que el nivel de riesgo sea LEVE, se asume el riesgo y no se establecen acciones de manejo, en caso contrario, siempre se deben establecer las acciones de manejo.

- **Fecha finalización de la acción:** Se establece fecha máxima en la cual se implementan las acciones de manejo.

- **Áreas involucradas en el manejo:** Se determinan las áreas involucradas, solo aplica, cuando el riesgo se comparte.

6.3.5 PRIMER SEGUIMIENTO GESTIÓN DE RIESGOS (Hoja 3 – Matriz de Riesgos)

6.3.6 SEGUNDO SEGUIMIENTO GESTIÓN DE RIESGOS (Hoja 4 – Matriz de Riesgos)

Los usuarios de la metodología realizan seguimiento a sus mapas de riesgos dos veces al año, con el fin de garantizar su pertinencia, control y actualización; verificando para cada riesgo:

- Medición y Análisis del Indicador: se realiza la medición, de acuerdo a la formula establecida en la hoja 2, y se realiza el análisis del indicador.
- Efectividad y Análisis de los controles: se realiza análisis sobre la efectividad en la aplicación de los controles.
- Efectividad y Análisis de las acciones de manejo: si existen acciones de manejo, se realiza la medición en cuanto al cumplimiento de las acciones y en cuanto a la eficacia de las mismas
    - Cumplimiento: Total / Parcial / No cumplida. Y se realiza el respectivo análisis.
    - Eficacia: Eficaz / No Eficaz / Pendiente de evaluación / Sin evaluación de la eficacia. De acuerdo al nivel de cumplimiento.
- Situación del riesgo luego del seguimiento: se selecciona la situación Riesgo controlado / Requiere nueva acción / Continua con la acción anterior.

Los auditores internos del Sistema Integral de Gestión, en el ejercicio anual de auditoría interna, evalúan la aplicación de la metodología.

- La actualización de los mapas de riesgos se realizará una vez al año o cuando por

cambios en el entorno o en el contexto interno se afecte las funciones de la Universidad.

- La materialización de riesgos conllevará a:

6.4 ETAPAS PARA LA CONSTRUCCIÓN DEL MAPA DE GESTIÓN DE RIESGOS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

6.4.1 INTRODUCCIÓN A LA MATRIZ DE RIESGOS SGSI.

El formato para la gestión de riesgos de seguridad de la información, se encuentra publicado en la página del Sistema Integral de Gestión, sí bien se cuenta con el mapa de gestión de riesgos (general), debido a la especificidad enmarcada dentro de la norma 27001:2022, así como los lineamientos de la función pública, se hace necesario implementar un instrumento, debido a la particularidad, importancia e impacto que se tiene en este proceso de identificación de riesgos, cabe mencionar que la metodología es muy similar, pero cambia en cuanto a la identificación de riesgos con base en los activos de información y las amenazas que se derivan de los mismos, también en la metodología de controles, los cuales se encuentran ya establecidos dentro de los anexos de la norma.

Los mapas de riesgos de Seguridad de la información y sus seguimientos deberán ser revisados, aprobados y posteriormente enviados por los jefes de las áreas de las Tecnologías Informáticas, mediante correo electrónico a la oficina del Sistema Integral de Gestión (SIG); se entenderá como aprobados con el envío del formato 1313-SIG-F64 Riesgos de Seguridad de la Información áreas del alcance.

6.4.2 ETAPAS EN LA CONSTRUCCIÓN DEL MAPA DE RIESGOS

- ***IDENTIFICACIÓN Y CLASIFICACIÓN DE LOS ACTIVOS DE INFORMACIÓN (Hoja 01)***
  Se diligencia la información contenida en el formato, en el cual se establecen los activos de información, y se categoriza según su nivel de: confidencialidad / Integridad / Disponibilidad / Criticidad del activo.
  Una vez diligenciado el inventario de activos (Información, Conocimiento, hardware, software o servicios), insumo principal para determinar aquellos activos de información con una criticidad alta (01. Inv. y clasificación activo). Con los activos de Criticidad alta se determina el nivel de vulnerabilidad que tiene el activo de información frente a una potencial amenaza.

- ***VULNERABILIDAD Y AMENAZA DEL RIESGO (Hoja 02)***
  Únicamente aquellos activos de información que obtienen un nivel de criticidad “Alta” migran a esta hoja, se les realiza el análisis de las vulnerabilidades y amenazas, identificando: tipo, descripción y probabilidad para cada una de ellas, posteriormente de

acuerdo al nivel de criticidad, se identifica el riesgo asociado al activo de información, finamente se define si el área va a dar tratamiento al riesgo para la presente vigencia.

- ***IDENTIFICACIÓN DEL RIESGO (Hoja 03)***
  En la hoja 3, una vez migran automáticamente los riesgos marcados con "SI" para ser trabajados en la presente vigencia (ver hoja 02), se procede a realizar la identificación, análisis, valoración, diseño de controles, y acciones de manejo, para cada uno de los riesgos identificados.

- ***SEGUIMIENTO 1 de 2 (Hoja 04)***
- ***SEGUIMIENTO 2 de 2 (Hoja 05)***

  Se realiza seguimiento a la gestión de riesgos de Seguridad de la información, dos veces al año. En cada seguimiento se revisa:

  - INDICADOR DEL RIESGO con su respectiva medición y análisis.
  - CONTROLES: dificultades en la aplicación del control
  - SITUACIÓN DEL RIESGO LUEGO DEL SEGUIMIENTO: determinando sí el riesgo está controlado, requiere nuevas acciones, o continua con la acción.

Los mapas de riesgos por proceso, serán publicados en la página web del Sistema Integral de Gestión, por temas de confidencialidad los riesgos de seguridad de la información se mantendrán como información reservada.

Para los riesgos relacionados con la seguridad de la información, los controles estarán enmarcados en los existentes en el Anexo A de la norma ISO/IEC 27001, seleccionando un TEMA y CONTROL a utilizar para evitar la materialización de los riesgos, revisar la tabla de Controles Anexo A – Norma ISO/IEC 27001, que se encuentra en el instructivo del formato Riesgos Seguridad de la Información áreas del alcance.

6.5 EVALUACIÓN AL MAPA DE RIESGOS

Control Interno será el órgano, quien a nivel interno se encargará de realizar dentro de sus ejercicios de auditoría, la EVALUACIÓN INDEPENDIENTE, ASESORA Y RECOMIENDA frente a la gestión de riesgos. Los resultados de esta evaluación serán presentados al Comité Institucional de Control Interno, con el fin de tomar decisiones respecto a las directrices relacionadas con los riesgos.

6.6 MATERIALIZACIÓN DE RIESGOS

En caso de materialización del riesgo, el responsable de la gestión del mismo, deberá diligenciar el formato de Toma de Acciones, de acuerdo a lo establecido en el mismo procedimiento.

Diligenciando Acción Correctiva con lo que precisa.

6.7 INCLUSIÓN DE CONTROLES, O ACCIONES DE MEJORA

Cuando, dentro de la vigencia, posterior a la actualización del mapa de riesgos, se identifican otros controles u otras acciones de manejo, estas ya no se incluirán en el mapa de riesgos de esa vigencia, si no, hasta la siguiente vigencia, sin embargo, para efectos de implementar dichas acciones y documentarlas, estas serán incluidas en formato de Toma de Acciones, de acuerdo a lo establecido en el mismo procedimiento. Diligenciando Acciones frente a un riesgo con lo que precisa

Elaborado Por:	Revisado Por:	Aprobado Por:
Personal UTP	Profesional Especializado III Gestión del Sistema Integral de Calidad	Director Administrativo grado 21 Vicerrectoría Administrativa y Financiera

**********Fin del documento**********