Versión: 10	Fecha: 2024-03-22	Código: SGC-PRO-011	Página: 1 de 14

ADMINISTRACIÓN DE RIESGOS

Contenido

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 administración de riesgos.

3. ABREVIATURAS / DEFINICIONES

a) **RIESGO:** Posibilidad de que ocurra un acontecimiento que afecte el logro de los objetivos y resultados de la Institución.

b) **ADMINISTRACIÓN DE RIESGO:** Es el conjunto de acciones que se deben seguir para autocontrolar los riesgos en la Universidad y sus procesos, 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

c) **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.

d) **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

e) **ASPECTOS AMBIENTAL:** Entorno en el cual opera la Universidad, incluyendo el aire, agua, suelo, recursos naturales, flora, fauna, seres humanos y sus interrelaciones.

f) **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.

g) **EFECTIVIDAD DEL CONTROL:** S**e** refiere a que la aplicación del control puede dar como resultado la prevención o mitigación del riesgo.

h) 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.

i) 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.

4. CONTENIDO

La gestión de riesgos en la Universidad Tecnológica de Pereira, se realizará de acuerdo a las directrices para la gestión de riesgos y el procedimiento que se formula en este documento.

4.1 REVISIÓN Y APLICACIÓN DE LA METODOLOGÍA

4.1.1 Revisión

El Comité Institucional de Control Interno revisará periódicamente y aprobará si es necesario las directrices y la metodología para la administración de riesgos, identificando los ajustes que sean necesarios; igualmente establecerá la estrategia de socialización de esta metodología.

Las directrices y la metodología serán presentadas al Comité Institucional de Control Interno.

4.1.2 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.
- El Sistema Integral de Calidad será el responsable de divulgar a todos los usuarios, la información correspondiente a las directrices y metodología.

4.2 ADMINISTRACIÓN DE RIESGOS

La administración de riesgos en la Universidad contempla la formulación de un mapa de riesgos, el cual está conformado por:

- Formato Mapa de Riesgos (SGC-FOR-011-01): identificación, análisis, controles y acciones de tratamiento del riesgo.
- Formato Plan de Mitigación para el Mapa de Riesgos (SGC-FOR-011-02): acciones para mitigar el riesgo, cuando el riesgo residual es alto, o cuando es moderado y el proceso considera pertinente dichas acciones.
- Formato Seguimiento al Mapa de Riesgos (SGC-FOR-011-03): seguimiento al 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.
- Para los Riesgos de Seguridad de la Información se cuenta con el formato 1313-F12 – (Riesgos de Seguridad de la Información áreas del alcance), donde se realiza el diligenciamiento del 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. La unidad organizacional o facultad donde pertenece este activo de información, podrá definir si dará tratamiento al riesgo para la vigencia en curso. Al definir el riesgo, el formato habilita la opción para que este sea planteado (02-Vulnerabilidad y Amenaza), ingresándolo automáticamente al mapa de riesgos de seguridad de la Información (03. Mapa de riesgos) y continúa con la metodología que tiene la institución para la gestión de riesgos.

Las matrices se elaboran, administran y visualizan, de acuerdo a:

- **Proceso/PDI/OEC**
- **Unidad organizacional / área**
- **Nombre del Pilar PDI**
- **Mapa Institucional, sí se prioriza en este o no.**

Los mapas de riesgos por proceso, serán publicados en la página web del Sistema Integral de Gestión.

4.2.1 Etapas para la construcción del Mapa de Riesgos

A. Identificación

1. **Establecimiento de Contexto:** En el análisis del contexto se determinan los factores internos y externos de acuerdo a las directrices para la gestión de riesgos, con lo cual se determinarán las causas de los riesgos.
2. **Caracterización de los riesgos:** Los usuarios identifican y describen los riesgos potenciales, los clasifican de acuerdo a tipo y evalúan sus consecuencias; el análisis de las causas que originan el riesgo se podrá realizar a través del diagrama causa y efecto, para lo cual tendrán en cuenta los factores internos y externos establecidos en el contexto.

   Los riesgos se pueden clasificar en diferentes tipos conforme a lo establecido en las directrices para la gestión del riesgo: Estratégico, Imagen, Operacional, Financiero, Contable, Cumplimiento, Tecnológicos, Corrupción, Información, Seguridad y Salud en el trabajo, Ambiental, Derechos Humanos.

B. Análisis

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

Según la probabilidad, se definen:

ALTO: Cuando su ocurrencia es casi segura. MEDIO
ALTO: Cuando su ocurrencia es probable. MEDIO:
Cuando su ocurrencia es posible.
MEDIO BAJO: Cuando su ocurrencia es improbable.

BAJO: Cuando es raro que se presente o no se ha presentado.

Según el impacto, se definen:

ALTO: Cuando las consecuencias del riesgo son catastróficas para la Universidad.

MEDIO ALTO: Cuando las consecuencias del riesgo son altas o mayores para la Universidad.
MEDIO: Cuando las consecuencias son moderadas para la Universidad.
MEDIO BAJO: Cuando las consecuencias tienen menor impacto para la Universidad.
BAJO: Cuando las consecuencias son insignificantes para la Universidad.

Al finalizar este análisis, se cruzan estas dos variables obteniendo la matriz de riesgo inherente así

CALIFICACIÓN DEL RIESGO INHERENTE

PROBABILIDAD								
	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
	IMPROBABLE	**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				

Para obtener la calificación del riesgo inherente, se deberá individualizar la escala de calificación de la probabilidad y el impacto para cada uno de los riesgos basado en la experticia, información objetiva y/o datos históricos, teniendo como base las tablas de análisis establecidas para tal fin (tablas No. 1 y No. 2 anexas).

C. Valoración

Los riesgos se valoran de acuerdo a los controles existentes, los cuales se pueden clasificar en:

- Control de dirección: permiten crear guías para el cumplimiento de los resultados.
- Control detectivo: permiten identificar si los resultados indeseables han ocurrido después de un acontecimiento.

- Control preventivo: permiten evitar o limitar la posibilidad de materialización de un riesgo.
- Control correctivo: permiten corregir los resultados indeseables que se han observado.

En esta etapa se deben evaluar los controles calificándolos de acuerdo a la situación en la cual estos se encuentren:

1) Documentados, aplicados y efectivos: Los controles existentes son aplicados, efectivos para la prevención o mitigación del riesgo y se encuentran documentados.
2) Aplicados, efectivos y No documentados: Los controles existentes aplicados y que son efectivos para la prevención o mitigación del riesgo no se encuentran documentados.
3) Aplicados y No efectivos: Los controles existentes que son aplicados no son efectivos para la prevención o mitigación del riesgo.
4) No aplicados: Los controles existentes no son aplicados por el responsable para la prevención o mitigación del riesgo.
5) No Existen controles: No existen controles asociados al riesgo para su prevención o mitigación.

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 un 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.

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:

CALIFICACIÓN DEL RIESGO RESIDUAL

PRIORIZACIÓN INICIAL							
		25	25	50	75	100	125
		20	20	40	60	80	100
		16	16	32	48	64	80
		15	15	30	45	60	75
		12	12	24	36	48	60
		10	10	20	30	40	50
		9	9	18	27	36	45
		8	8	16	24	32	40
		6	6	12	18	24	30
		5	5	10	15	20	25
		4	4	8	12	16	20
		3	3	6	9	12	15
		2	2	4	6	8	10
		1	1	2	3	4	5
			1	2	3	4	5
			FUERTE	ACEPTABLE	DEBIL		INEXISTENTE
			VALORACIÓN DEL CONTROL				

	ZONA GRAVE
	ZONA MODERADA
	ZONA LEVE

D. Manejo de 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:

- 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.

NIVEL EXPOSICIÓN RIESGO	OPCIÓN DE TRATAMIENTO	ACCIONES A TOMAR
GRAVE **Riesgos con calificación superior o igual a 36**	Evitar Reducir Transferir Compartir	Se deberá implementar inmediatamente las acciones preventivas que conlleven a evitar, reducir, transferir o compartir el riesgo de acuerdo al procedimiento de tomas de acciones SGC-PRO-006 del Sistema Integral de Gestión. Las acciones preventivas tomadas deberán conllevar a implementar nuevos controles que prevengan la materialización del riesgo y a mitigar el impacto. Se debe implementar el plan de contingencia frente a estos riesgos.
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 de acuerdo al procedimiento de tomas de acciones SGC-PRO-006 del Sistema Integral de Gestión. Se deberá implementar acciones preventivas que conlleven a mejorar el diseño o eficacia de los controles existentes. La implementación de un plan de contingencia estará sujeto a las necesidades del usuario de la metodología
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.

Se debe formular un indicador que permita monitorear el comportamiento del riesgo respecto al tratamiento y las acciones emprendidas para su manejo.

4.2.2 Acciones Preventivas

Se deben formular acciones preventivas de acuerdo al tratamiento seleccionado para los riesgos que se encuentren en los niveles de exposición grave y moderado.

Las acciones preventivas, son gestionadas de acuerdo al procedimiento de toma de acciones código (SGC-PRO-06).

4.2.3 Plan de mitigación.

Se formula el Plan de mitigación para los riesgos con nivel de exposición grave en el formato establecido.

En caso de que el riesgo quede en nivel de exposición moderada, cada usuario define si elabora plan de mitigación.

4.3 SEGUIMIENTO Y EVALUACIÓN A LA ADMINISTRACIÓN DE RIESGO

El seguimiento y evaluación a la administración de riesgos por parte de los usuarios se realiza conforme a lo establecido en las directrices para la gestión de riesgo.

Los usuarios de la metodología realizan seguimiento y evaluación a sus mapas de riesgos, con el fin de garantizar su pertinencia, control y actualización; para ello verifican los riesgos, la efectividad de los controles y la implementación de las acciones de tratamiento planteadas. La información se registra en el formato de Seguimiento del Mapa de Riesgos.

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

4.3.1 Seguimiento a la Gestión de Riesgos

4 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.

5 La revisión de la efectividad de los controles implementados, el seguimiento a los indicadores y las acciones propuestas, que se encuentren registrados en el mapa de riesgos, se revisarán dos veces al año.

6 La materialización de riesgos conllevará a:

- Ubicados en zona GRAVE de la matriz de riesgo residual, el responsable de la gestión de riesgos implementará de manera inmediata el plan de mitigación documentado, con el fin de que se dé continuidad a las actividades del proceso al servicio afectado. Así mismo, realizará los análisis respectivos sobre las fallas en los controles.
- Ubicados en zona MODERADA, el responsable de la gestión de riesgos implementará el plan de mitigación si este fue documentado. Así mismo, realizará los análisis respectivos sobre las fallas en los controles.
- Ubicados en zona LEVE, se deberán tomar acciones correctivas y el suceso deberá ser registrado al momento de realizar el seguimiento a los mapas de riesgos, por lo cual el responsable de la gestión de riesgos en el proceso evaluará los controles con el fin de determinar la eficacia y efectividad de los mismos y el nivel de vulnerabilidad.

4.3.2 Evaluación al Mapa de Riesgos Institucional

Control Interno deberá realizar dentro de sus ejercicios de auditoria, la evaluación de 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.

5. 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 el procedimiento establecidos por la Universidad para la gestión de riesgos. Realizar actualización y seguimiento a su mapa de riesgos 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 del procedimiento de acuerdo a las directrices definidas.

5. DOCUMENTOS DE REFERENCIA.

Directrices para la gestión de riesgos (SGC-INT-011-02)
Formato Mapa de riesgos (SGC-FOR-011-01).
Formato Plan de mitigación (SGC-FOR-011-02).
Formato seguimiento al mapa de riesgos (SGC-FOR-011-03).

Elaborado por:	Revisado por:	Aprobado por:
Personal UTP	**Directivo 21** **Vicerrector Administrativo y Financiero**	**Equipo para la Gestión de Riesgos**