ANEXO N°2 PROCESO DE GESTIÓN DE RIESGOS

UNIVERSIDAD DE LOS ANDES

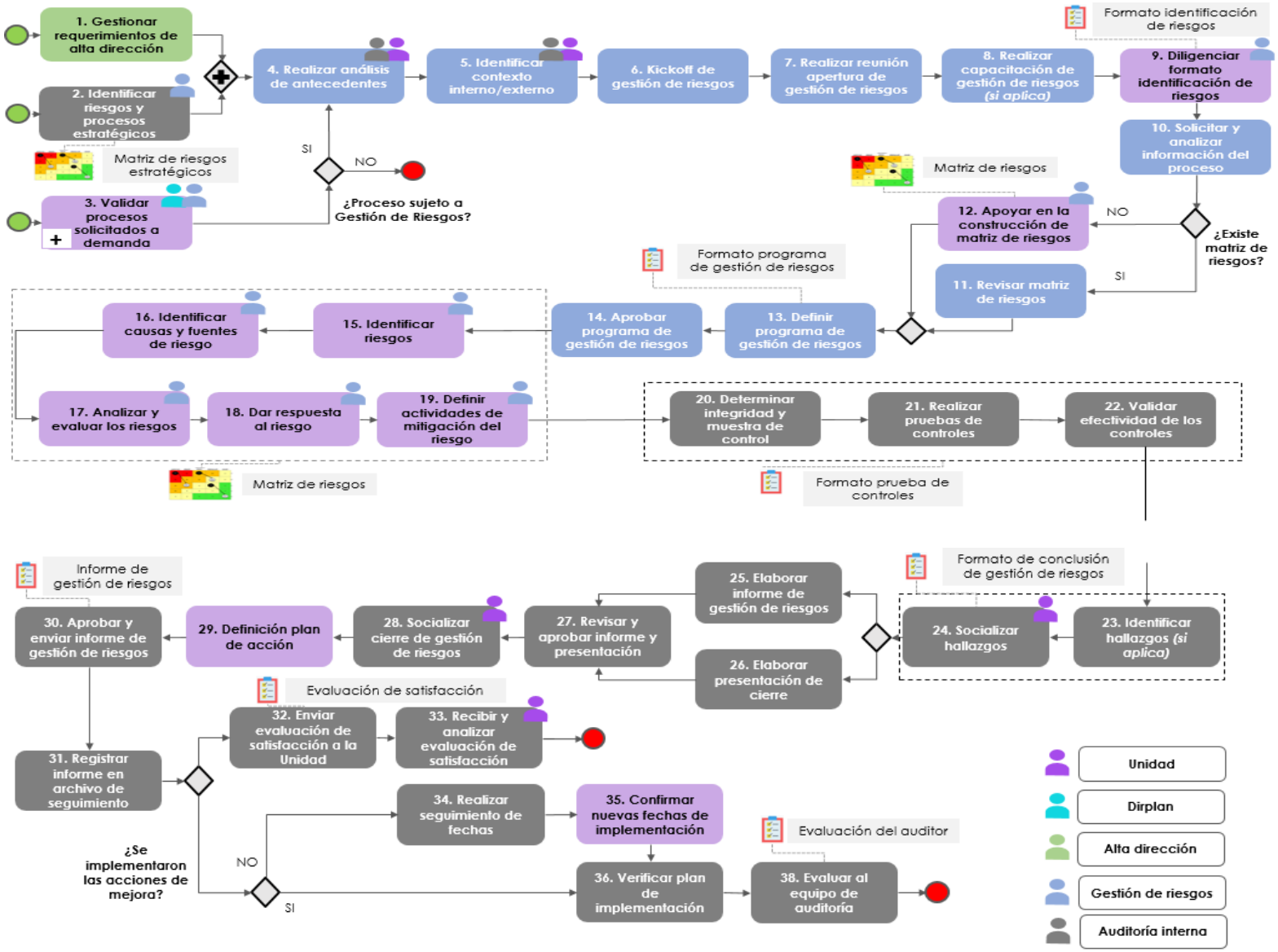
1.1. Proceso de gestión de riesgos operativos

El proceso de gestión de riesgos implica la aplicación sistemática de políticas y procedimientos que permiten la identificación, evaluación, tratamiento, seguimiento, comunicación y consulta de los riesgos. El proceso de la gestión del riesgo debe ser una parte integral de la gestión y toma de decisiones, la cual se debe integrar en la estructura, las operaciones y los procesos de la Institución a nivel operacional, de programa o de proyecto.

1.1.1. Ejecutar el proceso gestión de riesgos

Para implementar el proceso de gestión de riesgos en la Institución, se estableció mediante el siguiente esquema:

Gráfica 1. Proceso de gestión de riesgos


1. Gestionar requerimientos de alta dirección
2. Identificar riesgos y procesos estratégicos
Matriz de riesgos estratégicos
3. Validar procesos solicitados a demanda
4. Realizar análisis de antecedentes
5. Identificar contexto interno/externo
6. Kickoff de gestión de riesgos
7. Realizar reunión apertura de gestión de riesgos
8. Realizar capacitación de gestión de riesgos (si aplica)
9. Diligenciar formato identificación de riesgos
Formato identificación de riesgos
10. Solicitar y analizar información del proceso
¿Existe matriz de riesgos?
NO
SI
12. Apoyar en la construcción de matriz de riesgos
Matriz de riesgos
11. Revisar matriz de riesgos
¿Proceso sujeto a Gestión de Riesgos?
SI
NO
13. Definir programa de gestión de riesgos
14. Aprobar programa de gestión de riesgos
Formato programa de gestión de riesgos
15. Identificar riesgos
16. Identificar causas y fuentes de riesgo
17. Analizar y evaluar los riesgos
18. Dar respuesta al riesgo
19. Definir actividades de mitigación del riesgo
Matriz de riesgos
20. Determinar integridad y muestra de control
21. Realizar pruebas de controles
22. Validar efectividad de los controles
Formato prueba de controles
Informe de gestión de riesgos
30. Aprobar y enviar informe de gestión de riesgos
29. Definición plan de acción
28. Socializar cierre de gestión de riesgos
27. Revisar y aprobar informe y presentación
25. Elaborar informe de gestión de riesgos
26. Elaborar presentación de cierre
Formato de conclusión de gestión de riesgos
24. Socializar hallazgos
23. Identificar hallazgos (si aplica)
Evaluación de satisfacción
32. Enviar evaluación de satisfacción a la Unidad
33. Recibir y analizar evaluación de satisfacción
31. Registrar informe en archivo de seguimiento
34. Realizar seguimiento de fechas
35. Confirmar nuevas fechas de implementación
¿Se implementaron las acciones de mejora?
NO
SI
36. Verificar plan de implementación
Evaluación del auditor
38. Evaluar al equipo de auditoría
Unidad
Dirplan
Alta dirección
Gestión de riesgos
Auditoría interna

1.1.2. Planificación y evaluación del contexto.

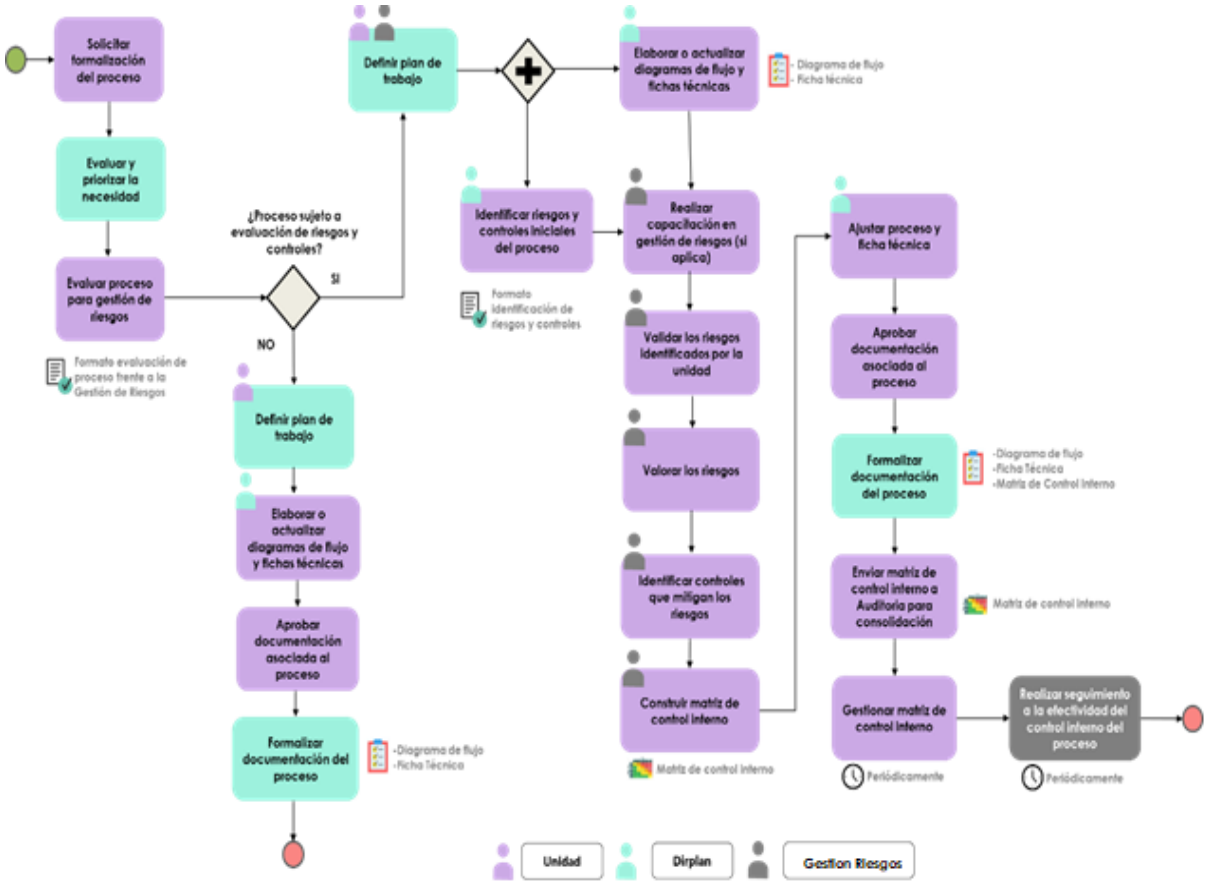
1.1.2.1. Gestión de requerimientos

La Unidad Responsable de la Gestión de Riesgos (URGR) o el Responsable de la Función de Gestión de Riesgos (RFGR) , recibe y gestiona las solicitudes requeridas por parte de las unidades como parte del levantamiento o revisión de procesos, relacionadas con actividades de gestión de riesgos. Estas solicitudes podrán recibirse en reuniones o por correo electrónico a la dirección gestionderiesgos@uniandes.edu.co.

1.1.2.2. Validar procesos solicitados a demanda

El RFGR y la Dirección de Planeación y Evaluación determinarán la pertinencia de realizar o no las actividades asociadas con el aseguramiento del Control Interno y Gestión de Riesgos Operativos como parte de la formalización de los procesos de las unidades académicas y administrativas de la Universidad.

La pertinencia será determinada por medio del diligenciamiento del formato FOR-45-1-01-13 Evaluación de proceso frente a la Gestión de Riesgos. A continuación, se establecen los responsables y las actividades generales a realizar para el aseguramiento del Control Interno y la Gestión de Riesgos en cada uno de los procesos:



Gráfica 2. Proceso gestión de riesgos Dirplan.

1.1.2.3. Realizar análisis de antecedentes

Una vez seleccionados los procesos que, por su nivel de impacto o relevancia para la Institución, requieran la implementación de un Sistema de Gestión de Riesgos, en primera instancia se debe realizar un análisis de antecedentes realizado por la Auditoria Interna, el RFGR o el Analista de Gestión de Riesgos y Control Interno, mediante las siguientes actividades:

- Revisión documental de papeles de trabajos, informes de auditoría o informes de gestión de riesgos anteriores.
- Revisión de la matriz de riesgos del proceso, si existe.
- Cambios en los procesos, políticas y normatividad aplicable.

Lo anterior permitirá identificar riesgos y aspectos relevantes que deban ser considerados.

1.1.2.4. Identificar contexto interno/externo

La unidad a cargo de la gestión de riesgos, en conjunto con el responsable de la función de gestión de riesgos y la unidad responsable del proceso, deberán analizar el contexto interno y externo en el cual opera el proceso o proyecto, para realizar una adecuada gestión de riesgo.

Por esto se analizarán aspectos como: la cultura Institucional, objetivos de los procesos, normatividad interna y externa, entre otros.

> Este contexto debe establecerse considerando los factores mencionados en el capítulo 2.1 sección ***2.1.1. Establecer liderazgo y compromisos de la alta dirección y*** *¡Error! No se encuentra el origen de la referencia.*.

1.1.2.5. Kickoff de gestión de riesgos

El responsable de la función de gestión de riesgos, realizará una reunión interna con el objetivo de discutir los aspectos relevantes que deben ser tenidos en cuenta para el desarrollo del proceso de gestión de riesgos, entre los cuales se encuentran:

- Definir el objetivo de la gestión de riesgos a realizar, con base en los siguientes criterios:
    - Expectativas de la Dirección
    - Conocimiento del proceso por parte del responsable de gestión de riesgos.
    - Necesidades planteadas por la unidad correspondiente.

- Establecer el alcance del proceso de gestión de riesgos.
- Definir los tiempos, la ubicación, las inclusiones y las exclusiones específicas.
- Identificar las herramientas y técnicas apropiadas para el desarrollo del proceso de gestión de riesgos.
- Establecer los recursos, responsables y documentación a conservar.

- Identificar si el proceso afecta o realiza actividades trasversales con otras unidades.
- Validar si en el proceso se han realizado cambios en cuanto a estructura, responsabilidades o ejecución de procedimientos.
- Contemplar las recomendaciones dadas, eventualmente, por parte de la Auditoría Interna en las reuniones de análisis de antecedentes y análisis de contexto interno/externo.

De esta reunión se definen los puntos clave que deben ser tenidos en cuenta para la realización de la reunión de apertura con la unidad correspondiente. Adicional se debe definir los puntos clave de la reunión y consignarlos en el formato acta de reuniones.

1.1.2.6. Realizar reunión apertura de gestión de riesgos

El Analista de Gestión de Riesgos y Control Interno (AGRyCI) o el RFGR, realizará una presentación a la unidad correspondiente, con base en las indicaciones establecidas en la reunión de Kickoff, donde se debe incluir:

- Objetivo.
- Alcance.
- Metodología establecida para la gestión de riesgos.
- Actividades o procesos a realizar.
- Tiempos de ejecución de la gestión de riesgos.
- Protocolo de comunicaciones.
- Equipo de gestión de riesgos definido.

1.1.2.7. Realizar capacitación de gestión de riesgos.

Con el objetivo de dar a conocer a todas las unidades académicas y administrativas, la metodología de gestión de riesgos para la (identificación, evaluación, tratamiento y monitoreo), si aplica, realizará una capacitación al dueño del proceso y demás involucrados en el mismo.

Esta capacitación proporcionara a las unidades el conocimiento necesario para realizar una autogestión de sus riesgos y controles, a su vez el

diligenciamiento de su respectiva matriz de riesgos, así como su posterior mantenimiento.

1.1.2.8. Diligenciar formato identificación de riesgos y controles

El dueño del proceso en conjunto con la persona responsable de ejecutar el mismo, contaran con el apoyo del Analista de Gestión de Riesgos y Control Interno (AGRyCI) o el RFGR para diligenciar el formato FOR-45-1-01-14 Identificación de riesgos y controles; el propósito del formato es realizar el entendimiento general del proceso, y a su vez permitir la identificación inicial de riesgos y controles.

A continuación, se relacionan las principales actividades a evaluar en el formato:

1. Operacional
   - Identificar las personas que intervienen en el proceso y sus funciones.
   - Validar si existe segregación de funciones y los niveles de revisión y aprobación.
   - Verificar si el personal se capacita continuamente.
   - Validar si existen situaciones que afectan el desarrollo de las funciones en el cumplimiento del objetivo del proceso.

2. Calidad de la información
   - Validar el tipo de información de entrada y salida del proceso
   - Verificar el entregable o producto final.
   - Verificar el cumplimiento de ley de protección de datos.
   - Identificar las herramientas tecnológicas utilizadas.
   - Validar el nivel de automatización del proceso.

3. Normatividad
   - Validar la normatividad interna (políticas, directrices, lineamientos) y externa (leyes, regulaciones) aplicada al proceso.

4. Riesgos y controles
   - Identificar riesgos y controles asociados al proceso.

1.1.2.8.1. Identificar riesgos

La unidad correspondiente deberá identificar los riesgos asociados al proceso con el apoyo del responsable de gestión de riesgos, validando en primera instancia los riesgos ya identificados si existe una matriz de riesgos previa.

Teniendo en cuenta que un riesgo es un evento que afecta o impide el cumplimiento de los objetivos del proceso, al momento de redactarlo se debe tener en cuenta los siguientes aspectos:

- Debe ser escrito en lenguaje común, para ser comprensible por cualquiera de los responsables de la gestión de riesgos.
- Debe responderse fácilmente ¿Qué perdida representa ese riesgo?

Ejemplo: fraude, multa, demanda, reporte, robo, sanción, etc.

- Debe ser redactado en forma negativa, utilizando sinónimos como: ausencia, inexistencia, errores, incumplimientos, falta, inadecuado, entre otros.

EJEMPLOS		
Objetivo del proceso: Gestión de compras Institucional	**Riesgos**	Compras a proveedores con precios mayores al promedio del mercado
		Contratación de proveedores vinculados con actividades ilícitas

Tabla 1- Ejemplo de redacción de riesgos

1.1.2.8.2. Identificar causas y fuentes de riesgo

Posterior a la identificación de los riesgos, la unidad con apoyo del responsable de la función de gestión de riesgos, deben comprender la naturaleza de los mismos, además de sus características que incluyen: la

fuente del riesgo, consecuencias, probabilidad de materialización y los escenarios posibles de donde se puede materializar.

Algunos de los ejemplos más comunes de causas o fuentes son:

- No contar o inadecuada aplicación de directrices, políticas o procedimientos.
- Inadecuada segregación de funciones (operación)
- Inadecuada asignación de roles y responsabilidades. (sistema)
- Falta de capacitación o formación al personal.
- Falta de supervisión o seguimiento a las actividades.
- Falta de un sistema o mecanismos que permitan realizar seguimiento a las actividades de control.

Debido a que un riesgo puede tener múltiples causas y consecuencias, afectando a múltiples objetivos, este paso debe ser correctamente documentado para un eficiente desarrollo de la gestión de riesgos, por ende, se recomienda analizar los siguientes factores:

- La probabilidad de los eventos y de las consecuencias.
- La naturaleza y la magnitud de las consecuencias.
- La complejidad y la interconexión.
- Los factores relacionados con el tiempo y la volatilidad.
- La eficacia de los controles existentes.
- Los niveles de sensibilidad y de confianza.

1.1.2.8.3. Analizar y valorar el riesgo

Se realizará la evaluación de los riesgos teniendo en cuenta la probabilidad de ocurrencia y el impacto potencial en caso de materializaron. Esta evaluación se realizará en el respectivo mapa de calor Institucional.

Para conocer el procedimiento completo del análisis y valoración de riesgos, ver numeral 2.2.2 Análisis y evaluación del riesgo.

1.1.2.8.4. Dar respuesta al riesgo

Con base en la calificación obtenida del riesgo inherente, para los diferentes riesgos asociados al proceso, se debe realizar una evaluación (respuesta al riesgo), mediante la selección de alguna de las siguientes categorías (evitar, perseguir, reducir, trasladar o aceptar). Esta categorización permite la priorización de los riesgos, la cual debe ser determinada y justificada por los diferentes dueños de los procesos.

Ver detalle en capítulo **¡Error! No se encuentra el origen de la referencia. ¡Error! No se encuentra el origen de la referencia.**.

1.1.2.8.5. Definir acciones de mitigación del riesgo

Se deberá realizar el diligenciamiento de la Fase 2 de la matriz de riesgos, identificando aquellos controles que mitigan la materialización de los riesgos. Ver detalle en capítulo 2.2.3 Actividades de control.

1.1.2.8.6. Determinar integridad y muestra de controles

Una vez definido los diferentes controles asociados al proceso, es importante que el dueño del proceso tenga claridad en la definición de su población y asegurar la integridad de la misma, debido a que, el analista de auditoría o el responsable de la función de gestión de riesgos (según aplique), deberán realizar una validación de esta integridad, haciendo uso del formato de pruebas de controles, donde se tendrá en cuenta la definición de objetivo, alcance y fuente de la información necesarios para la ejecución del control, además de los siguientes criterios:

- ¿La información de entrada del control es completa, entendible y veraz?
- ¿La información de entrada del control contiene algún tipo de cálculo, que pueda afectar la precisión de la información?
- ¿Se realizan modificaciones a la información de entrada? ¿cuáles?, y cómo asegura que estas modificaciones no afectan la precisión del control?

En caso de que la información no sea integra y precisa, el analista de auditoría o el responsable de la función de gestión de riesgos (según aplique), no podrán realizar la validación del control correspondiente, hasta asegurar la integridad.

Cuando la validación de la integridad represente alta complejidad, el DAI o el responsable de la función de gestión de riesgos (según aplique), determinarán si se realizan las pruebas o no del correspondiente control.

1.1.2.9. Realizar pruebas de controles

La realización de estas pruebas tiene como objetivo medir la efectividad y solidez de los controles definidos y estará a cargo de los responsables de la Gestión de Riesgos y el Control Interno, así como de la Auditoría Interna, dentro de los procesos establecidos por cada uno de estos frentes.

1.2. Proceso de gestión de riesgos estratégicos

En construcción.

1.3. Monitoreo y comunicación

El monitoreo y evaluación del Sistema de Gestión de Riesgos estará a cargo de la Dirección de Planeación y Evaluación, en la Gestión de Riesgos Operativos y Control Interno, y conjuntamente con la Dirección de Auditoría Interna en lo que se refiere a la Gestión de Riesgos Estratégicos que se desarrolla más adelante; no obstante, de los resultados de los encargos de auditoria que se adelanten.