METODOLOGÍA PARA LA ADMINISTRACIÓN DEL RIESGO DE LA UNIVERSIDAD DEL CAUCA - MARUC

Oficina de Planeación y Desarrollo Institucional
Noviembre de 2021

TABLA DE CONTENIDO

INTRODUCCIÓN

Para la Universidad del Cauca la Administración del Riesgo cobra importancia frente aquellas situaciones internas y externas generadoras de incertidumbre y que pueden afectar positiva o negativamente el logro de objetivos y metas institucionales. Ello hace imperativa la construcción de herramientas que permitan anticipar los eventos que generan un impacto nocivo sobre la gestión universitaria.

Al ser un componente estratégico del Modelo Integrado de Planeación y Gestión, la Administración del Riesgo con enfoque sistémico e integral, es un elemento clave de la planeación estratégica, que contribuye a mejorar la gestión de todos los procesos respecto de sus planes, programas y proyectos que aseguran el logro de las metas misionales.

METODOLOGÍA PARA LA ADMINISTRACIÓN DEL RIESGO EN LA UNIVERSIDAD DEL CAUCA – MARUC

OBJETIVO:

La Metodología para la Administración del Riesgo de la Universidad del Cauca –MARUC, orienta técnicamente la gestión del riesgo bajo un enfoque sistémico de operación y controles preventivos, que brinden una seguridad razonable a los procesos, frente a la incertidumbre que afecta el logro de los objetivos misionales y estratégicos.

MARCO NORMATIVO:

- Ley 87 de 1993 Sobre el ejercicio de Control Interno
- Ley 1474 de 2011 Estatuto anticorrupción.
- Decreto 1083 de 2015 Decreto Único Reglamentario del Sector de Función Pública.
- Decreto 1499 de 2017 Actualiza el Modelo Integrado de Planeación y Gestión-MIPG.
- Norma ISO 31000:2018 Para la Gestión del Riesgo.
- Lineamientos para la gestión de riesgos de seguridad digital en entidades públicas, MINTIC, Anexo 4 del 2018.
- Guía para la Administración del Riesgo y el Diseño de Controles para Entidades Públicas-Riesgos de Gestión, Corrupción y de Seguridad Digital V:5 DAFP 2020.

I. POLÍTICA DE ADMINISTRACIÓN DEL RIESGO

1. OBJETIVO

La Universidad del Cauca como Institución de Educación Superior, en conexión con su estrategia institucional alineada con la paz territorial, orienta la gestión del riesgo bajo un enfoque sistémico de operación y controles preventivos, que brindan una seguridad razonable frente a la incertidumbre que afecta el logro de los objetivos estratégicos y la calidad del servicio misional, a través de una metodología que identifica, valora, controla y monitorea los eventos potencialmente adversos, en garantía del fortalecimiento de los procesos, la transparencia en la gestión y la toma oportuna de decisiones.

2. ALCANCE:

Dada su transversalidad, la Administración del Riesgo abarca los procesos estratégicos, misionales, de apoyo y de evaluación; planes, programas y proyectos y sistemas de gestión.

3. RESPONSABILIDADES:

	Autoridad Responsable	Función
1	Consejo Superior	Aprobar la política de Administración del Riesgo.
2	Rector	Liderar la implementación de la Política de Administración del Riesgo.
3	Comité Institucional de Gestión del Desempeño y del Control Interno	Proponer la Política de Administración del Riesgo.
4	Coordinador de la Gestión de Seguridad Digital	Asesorar y acompañar a los procesos en la implementación de la Gestión del Riesgo de Seguridad Digital. Apoyar el seguimiento de los controles aplicados. Informar a la Dirección sobre el comportamiento de los Riesgos de seguridad digital y su variación.
5	Líderes de procesos, supervisores e interventores de contratos o proyectos, coordinadores de otros sistemas de gestión, comités de riesgos, comités de contratación	Identificar, valorar, tratar y monitorear los riesgos.
6	Jefe de la Oficina de Planeación y Desarrollo Institucional - OPDI	Coordinar técnicamente la aplicación de la metodología de Administración del Riesgo. Coordinar técnicamente la formulación de los riesgos. Consolidar y socializar el Mapa de Riesgos. Difundir la Política de Administración del Riesgo. Monitorear la implementación de la Política de Administración del Riesgo. Monitorear el Mapa de Riesgos.

7	Jefe de la Oficina de Control Interno - OCI	Asesorar en la metodología de la administración del riesgo. Realizar seguimiento a la gestión del riesgo y a la efectividad de los controles. Recomendar mejoras a la política de administración del riesgo.

3.1. RESPONSABILIDAD Y LÍNEAS DE DEFENSA:

El Modelo Integrado de Planeación y Gestión – MIPG plantea como estrategia de gestión del riesgo y control, el sistema de líneas de defensa, que busca asignar roles específicos y coordinar con eficacia y eficiencia la cobertura de los controles.

Proceso Responsable		Líneas de Defensa	Gestión del Riesgo	Roles
1	Gestión de la Dirección Universitaria	Estratégica	Identificar, valorar, tratar y monitorear los Riesgos.	Liderar la gestión del riesgo y establecer su política.
2	Gestión de la Planeación y Desarrollo Institucional	Primera y Segunda		Coordinar y monitorear la gestión del riesgo.
3	Gestión de la Calidad			
4	Supervisores e interventores de contratos o proyectos, coordinadores de otros sistemas de gestión, comités de riesgos, comités de contratación, entre otros.			
5	Gestión Académica	Primera		Identificar, valorar y monitorear los riesgos.
6	Gestión de la Investigación, Innovación e Interacción social.			
7	Gestión de Cultura y Bienestar.			
8	Gestión Administrativa y Financiera.			
9	Gestión del Control y Mejoramiento Continuo	Tercera		Asesorar en la metodología y evaluar la gestión del riesgo.

4. DIFUSIÓN DE LA POLÍTICA DE ADMINISTRACIÓN DEL RIESGO

La Política de Administración del Riesgo se difundirá a todos los procesos y subprocesos, a través de los canales de comunicación e información institucional, y en actividades de capacitación, inducción y reinducción lideradas por la Oficina de Planeación y de Desarrollo Institucional y la División de Gestión del Talento Humano.

5. TIPOLOGÍA DE RIESGOS

La Universidad del Cauca determina la tipología de los riegos de la siguiente manera:

Tipo de Riesgo		Relacionados con
1	Estratégicos	El cumplimiento de la misión, visión, objetivos y políticas.
2	Estilo de Dirección	La toma de decisiones gerenciales y la gestión de la dirección.
3	Operativos	La operación de los procesos y sus relaciones.
4	Financieros	La administración de bienes y todas aquellos procesos involucrados con el proceso financiero como presupuesto, tesorería, contabilidad, cartera, central de cuentas, costos, etc.
5	Tecnológicos	La infraestructura y capacidad tecnológica.
6	Cumplimiento	Acatamiento de normas, principios, valores y la calidad del servicio, así como procesos contractuales y litigios judiciales.
7	Imagen	El buen nombre y la confianza en la institución.
8	Corrupción	El interés público y los principios de la función pública.
9	Seguridad Digital	Integridad, confidencialidad y disponibilidad de la información.
10	Ambientales	El medio ambiente, los recursos naturales no renovables.
11	Académicos	La calidad del servicio misional.

6. IMPACTO Y PROBABILIDAD

Para medir el impacto y probabilidad se definen las siguientes escalas:

Impacto	Probabilidad
Insignificante	Rara vez
Menor	Improbable
Moderado	Posible
Mayor	Probable
Catastrófico	Casi Seguro

6.1. ESCALA DE IMPACTO RIESGOS DE CORRUPCIÓN

La escala de impacto en los riesgos de corrupción, se maneja desde el nivel 3 en adelante, dado que son inaceptables.

6.2. VALORACIÓN DEL RIESGO

Para efectos de la valoración del riesgo, se relacionará la probabilidad de ocurrencia en términos de frecuencia y factibilidad, y el impacto a los objetivos misionales y de los procesos, determinando en la siguiente escala:

Nivel de Riesgo	Puntaje
Bajo	1-3
Medio	4-9

Alto	10-24
Extremo	25-100

7. TRATAMIENTO AL RIESGO

Para efectos de los niveles de tolerancia, de acuerdo con el impacto que su materialización generaría a los procesos, se considerará la siguiente escala:

Nivel de Riesgo	Nivel de Tolerancia
Bajo	Aceptable
Medio	Moderado
Alto	Importante
Extremo	Inaceptable

7.1. TRATAMIENTO

Conforme a su nivel de tolerancia se efectuará su tratamiento bajo los siguientes criterios:

Nivel de Tolerancia	Acciones	Descripción
Aceptable	Se asume el riesgo	No se toma ninguna acción; sin embargo, puede aplicarse un control como alternativa, analizando su relación costo beneficio.
Moderado	Se evita el riesgo.	Se abandonan los procedimientos generadores del riesgo, como alternativa excepcional.
Aceptable, Moderado, Importante e Inaceptable.	Se reduce el riesgo	Se adoptan nuevos controles o revalúan los existentes.
Importante, Inaceptable	Se comparte el riesgo	Transfiere el riesgo a terceros a través de contratos.

7.2. TRATAMIENTO RIESGOS DE CORRUPCIÓN

Siempre serán inaceptables los riesgos de corrupción, por lo que la Universidad impulsará estrategias y acciones para evitarlos, reducirlos y/o compartirlos.

8. SEGUIMIENTOS A LOS RIESGOS

La Oficina de Control Interno hará un seguimiento a la administración del riesgo, de la siguiente manera:

- Cuatrimestral, frente a la formulación del riesgo, el cumplimiento y la efectividad de los controles.
- Eventual, en la ejecución de las auditorías planteadas en el Programa de Auditoría, frente a cada proceso evaluado.

9. DEFINICIONES

Para efectos de la aplicación de la Política se tendrán en cuenta las siguientes nociones:

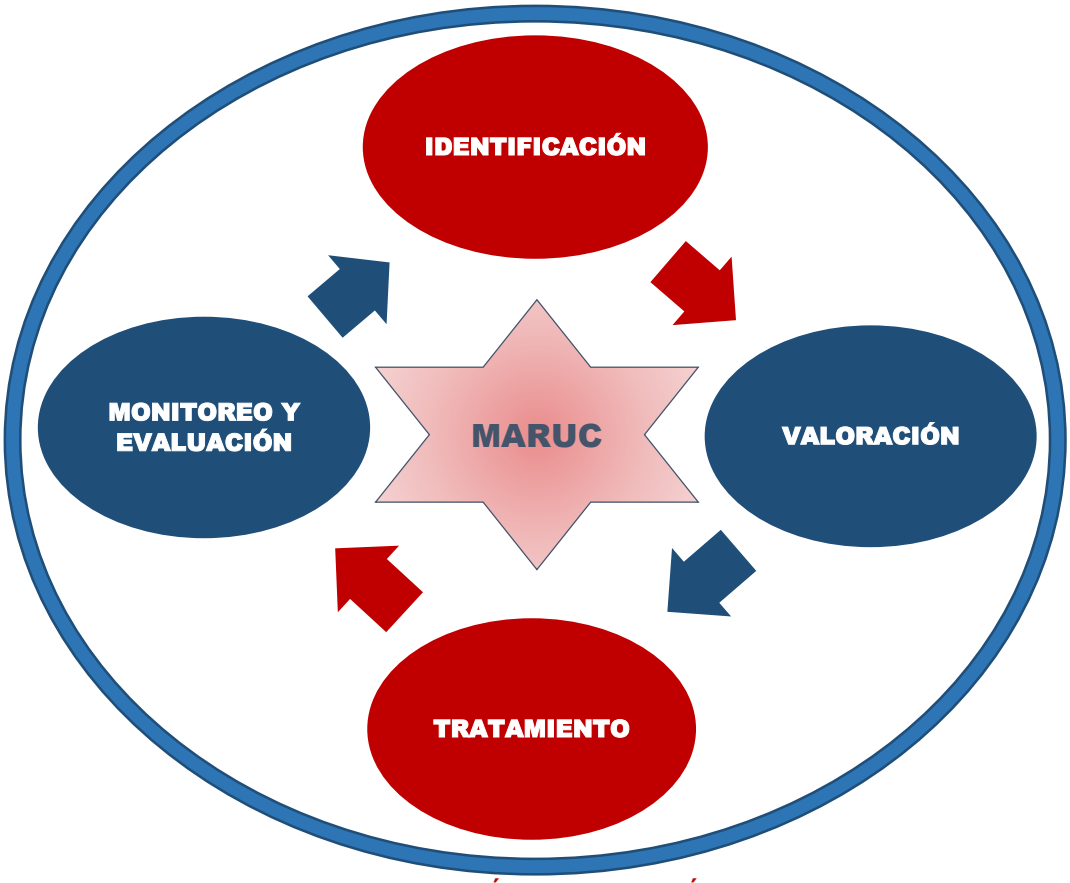
a. Activo de seguridad digital: Son aplicaciones, servicios web, redes, hardware, información física o digital y recurso humano que operan en el entorno digital.
b. Administración del Riesgo: Actividades coordinadas para gestionar el riesgo.
c. Amenaza: Hecho natural o humano que puede afectar negativamente a la Institución
d. Apetito al riesgo: Magnitud del riesgo que la Universidad está dispuesta a aceptar, asumir o evitar.
e. Causa: Factores internos y externos que contribuyen a materializar un riesgo.
f. Consecuencia: Resultado de la materialización del riesgo.
g. Control: Medidas para gestionar los riesgos.
h. Evento: Hecho que puede generar un riesgo.
i. Impacto: Magnitud en que afecta la materialización de un riesgo.
j. Mapa de riesgos: Representación consolidada de los riesgos.
k. Probabilidad: Posibilidad de ocurrencia del riesgo.
l. Riesgo: Efecto de la incertidumbre sobre los objetivos.
m. Riesgo de Corrupción: Posibilidad de ocurrencia de un evento adverso, por acción u omisión, que afecte el cumplimiento de los objetivos institucionales, y genere una desviación de lo público en beneficio personal o particular.
n. Riesgo inherente: Es el que se presenta sin controles.
o. Riesgo residual: Es el que permanece después de la aplicación de los controles
p. Tolerancia al riesgo: Niveles aceptables de desviación relativa a la consecución de objetivos.
q. Vulnerabilidad: Representa la debilidad de un activo o de un control que puede ser provechada por una o más amenazas.

II. METODOLOGÍA DE ADMINISTRACIÓN DEL RIESGO

CICLO DE LA ADMINISTRACIÓN DEL RIESGO:

Define la secuencia de actividades en la Administración del Riesgo de la Universidad del Cauca.

Ilustración 1. Etapas del Ciclo de la Administración del Riesgo.

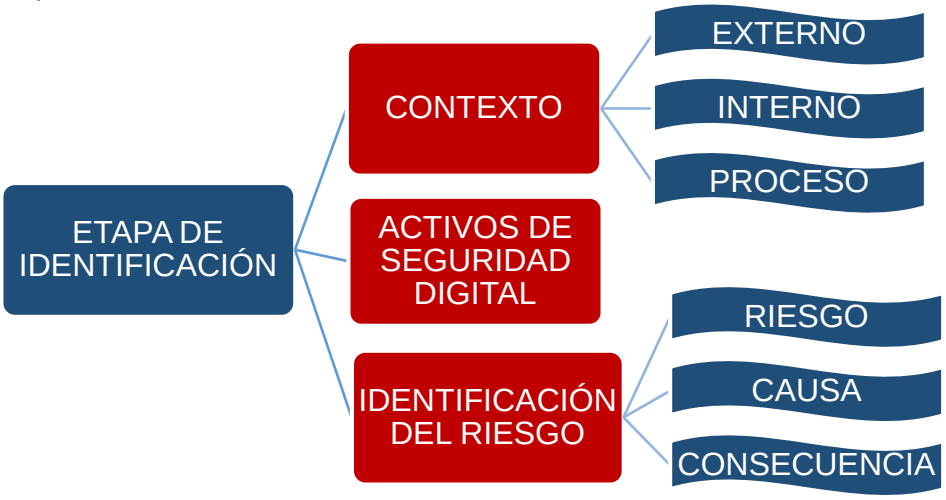


Fuente: Elaboración propia.

1. ETAPA DE IDENTIFICACIÓN

En la etapa de Identificación se determinan fuentes o factores, causas, consecuencias de riesgos, y se identifica el riesgo basado en datos históricos, análisis de datos, experiencias y necesidades de los procesos o subprocesos, teniendo en cuenta los objetivos estratégicos y los de su caracterización.

Ilustración 2. Etapa de identificación.



Fuente: Elaboración propia

1.1. CONTEXTO:

Es necesario identificar los objetivos estratégicos y los de la caracterización, del proceso o subproceso, con el fin de comprender los aspectos internos y externos que influyen en la configuración de un riesgo.

1.1.1. Contexto Externo de la Universidad:

Son las oportunidades y amenazas que afectan a la Institución o al proceso, conforme a las siguientes definiciones:

- Oportunidades: Son circunstancias ajenas al proceso, que pueden beneficiar el logro de sus objetivos.
- Amenazas: Situaciones ajenas al proceso, que pueden impedir el logro de sus objetivos.

Tabla 1. Factores Externos.

Externo	
Políticos	Cambios de gobierno, políticas públicas, orden público.
Económicos	Disminución del Presupuesto, recursos especiales (regalías), sanciones y condenas pecuniarias.
Sociales y Culturales	Responsabilidad social, zonas marginales, poblaciones vulnerables, estímulos educativos.
Tecnológicos	Conectividad, infraestructura y tecnología de punta, seguridad informática.
Ambientales	Catástrofes naturales, desarrollo sostenible, generación residuos.
Legales y reglamentarios	Leyes, regulaciones, lineamientos.

Fuente: Construcción propia adaptada de la Guía para la Administración del Riesgo y el diseño de controles en entidades públicas. DAFP V: 5 diciembre 2020.

1.1.2. Contexto Interno de la Universidad.

Son las fortalezas y debilidades que afectan a la Institución o al proceso, de acuerdo a los siguientes conceptos:

- ❖ Fortalezas: Son las condiciones que aumentan la capacidad del proceso en el logro de sus objetivos.
- ❖ Debilidades: Son insuficiencias que disminuyen la capacidad del proceso en el logro de sus objetivos.

Tabla 2. Factores Internos.

Interno	
Talento Humano	Competencias, relevo generacional, selección, ética, evaluación del desempeño, salud, seguridad, clima organizacional.
Infraestructura	Disponibilidad de áreas físicas
	Recursos tecnológicos
	Equipamiento.
Procesos	Misional: Diseño curricular, evaluación, acreditación de programas, proveedores de información, admisiones,
	Administrativo: información y comunicación, contratación, manejo de recursos.
Estratégicos	Estilo de dirección, planeación institucional, liderazgo, cumplimiento de objetivos, liderazgo, control social.
Activos de seguridad	Información, aplicaciones, hardware

Fuente: Construcción propia adaptada de la Guía para la Administración del Riesgo y el diseño de controles en entidades públicas. DAFP V: 5 diciembre 2020.

1.1.3. Contexto del proceso:

Son particularidades actuales del proceso reconocido en el Mapa de Procesos.

Tabla 3. Factores del Proceso.

Proceso	
Naturaleza	Estratégico, misional, de apoyo, evaluación.
Objetivo y alcance	Claridad en la descripción del alcance y objetivo.
Interacciones con otros procesos	Relación precisa con otros procesos en cuanto a insumos, proveedores, productos, usuarios o clientes.
Transversalidad	Procesos que determinan lineamientos necesarios para el desarrollo de todos los procesos de la entidad.
Procedimientos asociados	Pertinencia en los procedimientos que desarrollan los procesos.
Responsables del proceso	Grado de autoridad y responsabilidad de los funcionarios frente al proceso.

Comunicación entre los procesos	Efectividad en los flujos de información determinados en la interacción de los procesos
Activos de seguridad digital del proceso	Información, aplicaciones, hardware, y otros, que se deben proteger para garantizar el funcionamiento interno de cada proceso.

Fuente: Construcción propia adaptada de la Guía para la Administración del Riesgo y el diseño de controles en entidades públicas. DAFP V: 5 diciembre 2020.

1.1.4. Análisis DOFA:

Los datos más relevantes de cada contexto se organizan en la herramienta de diagnóstico DOFA, con el fin de relacionar las debilidades, fortalezas, amenazas y oportunidades. Las debilidades y amenazas que no se logren compensar con las fortalezas y oportunidades, se tendrán como causa de riesgos.

Tabla 4. Matriz DOFA

Factores	Positivos	Negativos
Externos (Del entorno)	Oportunidades	Amenazas
Internos (De la Entidad)	Fortalezas	Debilidades
Internos (Del Proceso)	Fortalezas	Debilidades

Fuente: Construcción propia adaptada de la Guía para la Administración del Riesgo y el diseño de controles en entidades públicas. DAFP V: 5 diciembre 2020.

1.2. ACTIVOS DE SEGURIDAD DIGITAL

Son elementos de la organización como aplicaciones, servicios web, redes, información física o digital, tecnologías de información -TI- y tecnologías de operación –TO, que utiliza para funcionar en el entorno digital.

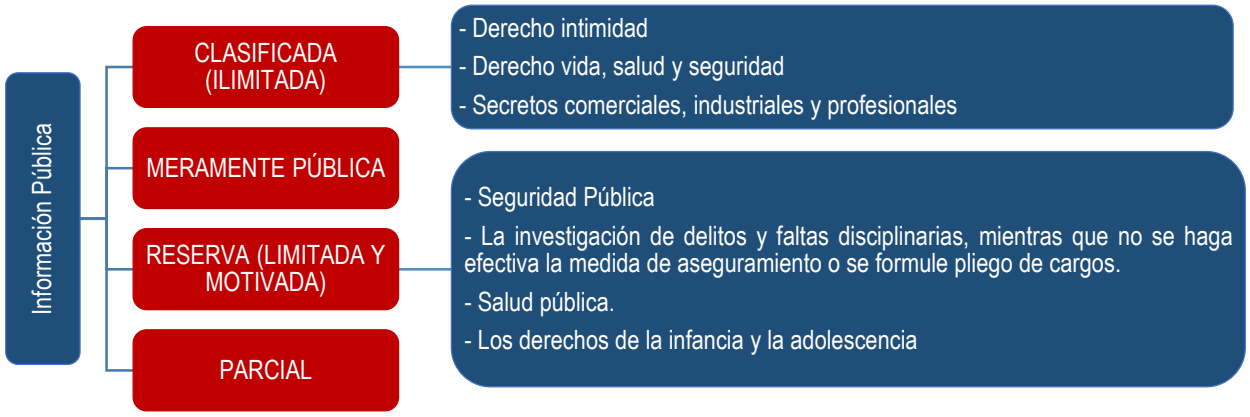
La identificación y valoración de activos se debe realizar por la Primera Línea de Defensa – Líderes de Proceso, siendo debidamente orientados por el responsable de seguridad digital o de seguridad de la información de la Universidad[1].

1.2.1. Tipología de la información

Los activos de Seguridad Digital custodian la información conforme a su tipología.

[1] Departamento Administrativo de la Función Pública – DAFP. Lineamientos para la Gestión de Riesgos de Seguridad Digital en Entidades Públicas. 2020, Pág. 11.

Ilustración 3. Tipología de la Información.



Fuente: Construcción propia, basado en las Leyes 1712 de 2014 y 1581 de 2012 y Decreto UR. 1081 de 2015 Planeación Nacional

1.2.2. Tipos de Activos

El Gobierno Nacional clasifica los activos en los siguientes grupos:

Tabla 5. Tipología de Activos

Tipo	Descripción
Información	Información almacenada en formatos físicos (papel, carpetas, CD, DVD) o en formatos digitales o electrónicos (ficheros en bases de datos, correos electrónicos, archivos o servidores), teniendo en cuenta lo anterior, se puede distinguir como información: Contratos, acuerdos de confidencialidad, manuales de usuario, procedimientos operativos o de soporte, planes para la continuidad del negocio, registros contables, estados financieros, archivos ofimáticos, documentos y registros del sistema integrado de gestión, bases de datos con información personal o con información relevante para algún proceso (bases de datos de nóminas, estados financieros) entre otros.
Software	Activo informático lógico como programas, herramientas ofimáticas o sistemas lógicos para la ejecución de las actividades.
Hardware	Equipos físicos de cómputo y de comunicaciones como, servidores, biométricos que por su criticidad son considerados activos de información.
Servicios	Servicio brindado por parte de la entidad para el apoyo de las actividades de los procesos, tales como: Servicios WEB, intranet, CRM, ERP, Portales organizacionales, Aplicaciones entre otros (Pueden estar compuestos por hardware y software).
Intangibles	Se consideran intangibles aquellos activos inmateriales que otorgan a la entidad una ventaja competitiva relevante, uno de ellos es la imagen corporativa, reputación o el good will, entre otros.
Componentes de Red	Medios necesarios para realizar la conexión de los elementos de hardware y software en una red, por ejemplo, el cableado estructurado y tarjetas de red, routers, switches, entre otros.

Personas	Aquellos roles que, por su conocimiento, experiencia y criticidad para el proceso, son considerados activos de información, por ejemplo: personal con experiencia y capacitado para realizar una tarea específica en la ejecución de las actividades.
Instalaciones	Espacio o área asignada para alojar y salvaguardar los datos considerados como activos críticos para la empresa.

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones

1.2.3. Criticidad del Activo

Dependiendo de su valor respecto de la confidencialidad, integridad y disponibilidad, se valora ALTA (3), MEDIA (2) y BAJA (1) y se promedia para encontrar su nivel.

Elementos para su construcción: Activo, Tipo, Confidencialidad, Integridad, Disponibilidad y Nivel

1.2.4. Identificación del Activo

Una vez determinados los elementos necesarios para la identificación del Activo es importante describirlo, definir sus responsables y armonizarlo con su tipología, clasificación y nivel criticidad, lo que permitirá establecer la prioridad en su gestión y su incidencia en la gestión del riesgo.

Elementos para su construcción: Proceso, Activo, Descripción, Responsable, Tipo, Clasificación y Criticidad

1.3. IDENTIFICACIÓN DEL RIESGO

La identificación de los riesgos depende de la tipología, no obstante, es importante tener en cuenta que todos ellos surgen a partir del análisis del contexto, el cual estará asociado a aquellos eventos o situaciones que pueden entorpecer el normal desarrollo de los objetivos estratégicos y del Proceso.

Los objetivos del proceso entendidos como los resultados esperados para lograr cumplir con la misión y visión institucional, que se relacionan directamente con las políticas institucionales y el quehacer de las dependencias.

Los riesgos que se identifiquen deben tener impacto en el cumplimiento del objetivo estratégico, del proceso o de la dependencia.

Los objetivos deben contener “qué”, “cómo”, “para qué”, “cuándo” y “cuánto”, si no se cuenta con una correcta definición de objetivos, no se puede determinar los riesgos de manera correcta.

La identificación se define de la siguiente manera:

Ilustración 4. Identificación del riesgo.

Fuente: Elaboración propia.

1.3.1. Riesgo:

Para una adecuada identificación del riesgo, se debe tener en cuenta lo siguiente:

- Relacione el riesgo con el objetivo estratégico, del proceso y/o subproceso.
- Evite definir la causa o el problema como riesgo: “Falta de”, “Debilidad”, “Deficiencia”.
- Evite expresar el riesgo como un incumplimiento o no conformidad.
- Se puede efectuar una imagen mental de su materialización.
- No describa el riesgo como omisiones, desviaciones o negaciones de un control.
- Inicia con verbo en sustantivo, por lo general con los sufijos ción, sión y cción, en los riesgos de corrupción pueden establecerse con verbos en infinitivo.

1.3.1.1. Origen del riesgo:

Puede estar asociado a las siguientes categorías:

Tabla 6. Categoría de riesgos:

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.

Fuente: Construcción propia adaptada de Guía para la administración del riesgo y el diseño de controles en entidades públicas. Versión 5. diciembre 2020

Conforme a su especialidad el riesgo se identifica de la siguiente forma:

- Riesgos de Gestión: Posibilidad de ocurrencia de algún evento que impacte el cumplimiento de los objetivos.

Elementos para la construcción del riesgo de gestión: Descripción del riesgo y relación con objetivo.

- Riesgos de corrupción: Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado. Requiere que se presenten 4 condiciones: (Acción/omisión + Uso del poder + Desviación de la gestión de lo público + Beneficio particular). Debe tenerse en cuenta los eventuales riesgos de corrupción a los que está expuesta la Universidad, analizando riesgos materializados en entidades semejantes.

  Esta tipología de riesgo puede estar asociada al conflicto de intereses el cual refiere a cualquier relación que tiene un servidor que vaya o parezca ir en contra del mejor interés de la organización; que puede menoscabar la capacidad de una persona para desempeñar sus obligaciones y responsabilidades de manera objetiva.

Elementos para la construcción del riesgo de corrupción: Descripción del riesgo, Acción/Omisión, Uso del poder, Desviación de la gestión pública y Beneficio particular

- Riesgos de Seguridad Digital: Afectan alguno de los tres (3) criterios de un activo (s) dentro del proceso: integridad, confidencialidad o disponibilidad.

Elementos para la construcción del riesgo de seguridad digital: Descripción del riesgo, Integridad, Confidencialidad y Disponibilidad

1.3.2. Causas:

En la identificación del Riesgo la determinación de causas es el resultado del análisis de los factores DOFA, y/o de la aplicación de técnicas de análisis de causas, puede identificarse más de una causa por riesgo priorizando las de mayor impacto.

En el contexto universitario se pueden presentar las siguientes causas:

Tabla 7. Referentes de Causas.

Causa
Falta de procedimientos
Controles deficientes en recaudos o aplicación de dineros públicos.
Manejo indebido de información privilegiada
Escala salarial por debajo del promedio de otras instituciones.
Manejo de turnos de manera discrecional
Exceso de actividades y de funcionarios que intervienen en la relación con el ciudadano.
Deficiencias de información o complejidad de los procedimientos
Mecanismos deficientes de registros de los documentos aportados para un trámite o procedimiento.
Falta de capacitaciones, inducciones y reinducciones.
No existen mecanismos documentados para verificar los requisitos acreditados para un procedimiento o un trámite.
Relaciones de amistad de entre usuarios y ejecutores de trámites y procedimientos.
Mecanismos incipientes de monitoreo a los trámites y procedimientos.
Autonomía profesional para el análisis de requisitos
Manipulación de decisiones o decisiones por encima de los conceptos técnicos
Excesiva reserva de la información sobre trámites y procedimientos
Ausencia de mecanismos sobre la discrecionalidad de quien tiene a cargo un trámite o procedimiento.
Inexisten de banco de conceptos técnico – jurídicos que frenen la interpretación subjetiva de las normas o reglamentos
Actores internos o externos de presión a las decisiones institucionales.
Falta de gestión de los líderes de los procesos que coordinan.
Los servidores desconocen los procedimientos que ejecutan.
Los servidores intervienen en procedimientos o trámites ajenos a su competencia funcional.
Trámites y procedimientos ejecutados manualmente.
Fallas en la cultura de la integridad y la probidad.
Asignación de funciones de naturaleza permanente a personal con vinculación transitoria.
Caídas de redes, aplicaciones y/o errores en los softwares
Desastres naturales como derrumbes, incendios e inundaciones
Suplantación de identidad
Hurtos y atentados contra el orden público

Fuente: Construcción propia

1.3.2.1. Causas en los riesgos de corrupción

Por su especial tratamiento, en los riesgos de corrupción se determinan de acuerdo con el triángulo de corrupción: I- presión, II- responsabilidad y III- oportunidad.

Ilustración *5*. Causas de los riesgos de corrupción.

Fuente: Adaptada de la Guía IGA- Procuraduría General (AL, 2012) - basada en Donald R. Cressey

❖ Causas en los riesgos de corrupción en trámites administrativos

En los trámites y procedimientos se presenta los riesgos de corrupción y sus causas de acuerdo con sus etapas:

Tabla 8. Referentes de causas en trámites administrativos.

Etapa	Riesgo	Oportunidad/Causa
Divulgación del trámite o procedimiento	Conformación de redes de intermediarios de procedimientos o trámite.	Información imprecisa del trámite o procedimiento
Radicación de documentos	Se acude a intermediarios para agilizar los tiempos de radicación y respuesta. Se concede prelación de turnos.	Demora en tiempos de atención o se atiende por fuera de turnos. Registros manuales.
Revisión de documentos y anexos	Ejecución de trámites o procedimientos sin el cumplimiento de requisitos legales o reglamentarios. Apropiación de los pagos que generan los trámites. Se realizan pagos por debajo de la tarifa oficial Aceptación de documentos con información adulterada.	Recaudos directos sin registros. Falta de mecanismos de verificación.

Etapa	Riesgo	Oportunidad/Causa
Gestión de la solicitud	Aplicación de criterios flexibles para lograr trámites y procedimientos, a cambio de dádivas. Alteración de documentos recibidos para el cumplimiento de requisitos de un trámite o procedimiento.	Contacto informal entre ejecutores de un procedimiento o trámite y usuarios. Autonomía en la aplicación de criterios técnicos del operador del trámite o procedimiento.
Otras		

Fuente: elaboración propia con base: Protocolo para la Identificación de Riesgos de Corrupción asociados a la prestación de trámites y servicios del DAFP.

1.3.2.2. Causas (vulnerabilidad) y amenazas en los riesgos de Seguridad Digital

Las causas se analizan de acuerdo a la vulnerabilidad y la amenaza que representa.

- Vulnerabilidad: Son aquellas debilidades que se presentan sobre los activos de información dependiendo de su tipología.

Tabla 9. Vulnerabilidad

Tipo	Vulnerabilidad
Hardware	Mantenimiento insuficiente
	Ausencia de esquemas de reemplazo periódico
	Sensibilidad a la radiación electromagnética
	Susceptibilidad a las variaciones de temperatura (o al polvo y suciedad)
	Almacenamiento sin protección
	Falta de cuidado en la disposición final
	Copia no controlada
Software	Ausencia o insuficiencia de pruebas de software
	Ausencia de terminación de sesión
	Ausencia de registros de auditoría
	Asignación errada de los derechos de acceso
	Interfaz de usuario compleja
	Ausencia de documentación
	Fechas incorrectas
	Ausencia de mecanismos de identificación y autenticación de usuarios
	Contraseñas sin protección
	Software nuevo o inmaduro
Red	Ausencia de pruebas de envío o recepción de mensajes
	Líneas de comunicación sin protección
	Conexión deficiente de cableado
	Tráfico sensible sin protección
	Punto único de falla
Personal	Ausencia del personal
	Entrenamiento insuficiente

Tipo	Vulnerabilidad
	Falta de conciencia en seguridad
	Ausencia de políticas de uso aceptable
	Trabajo no supervisado de personal externo o de limpieza
Lugar	Uso inadecuado de los controles de acceso al edificio
	Áreas susceptibles a inundación
	Red eléctrica inestable
	Ausencia de protección en puertas o ventanas
Organización	Ausencia de procedimiento de registro/retiro de usuarios
	Ausencia de proceso para supervisión de derechos de acceso
	Ausencia de control de los activos que se encuentran fuera de las instalaciones
	Ausencia de acuerdos de nivel de servicio (ANS o SLA)
	Ausencia de mecanismos de monitoreo para brechas en la seguridad
	Ausencia de procedimientos y/o de políticas en general (esto aplica para muchas actividades que la entidad no tenga documentadas y formalizadas como uso aceptable de activos, control de cambios, valoración

Fuente: ISO/IEC 27005

- Amenazas: Representan situaciones o fuentes que pueden hacer daño a los activos y materializar los riesgos.

Tabla 10. Amenaza

Tipo	Amenaza
Daño físico	Fuego.
	Agua.
Eventos naturales	Fenómenos climáticos.
	Fenómenos sísmicos
Pérdidas de los servicios esenciales	Fallas en el sistema de suministro de agua
	Fallas en el suministro de aire acondicionado
Perturbación debida a radiación	Radiación electromagnética
	Radiación térmica
Compromiso de la información	Interceptación de servicios de señales de interferencia comprometida
	Espionaje remoto
Fallas técnicas	Fallas del equipo
	Mal funcionamiento del equipo
	Saturación del sistema de información
	Mal funcionamiento del software
	Incumplimiento en el mantenimiento del sistema de información
Acciones no autorizadas	Uso no autorizado del equipo
	Copia fraudulenta del software
Compromiso de las funciones	Error en el uso o abuso de derechos
	Falsificación de derechos

Fuente: ISO/IEC 27005:2009

1.3.3. Consecuencia

Es el efecto de la materialización del riesgo, que puede acarrear responsabilidades tales como: legal, penal, disciplinaria, fiscal, social, de confianza, imagen, estructural, pérdida de información.

1.3.4. Formatos de Identificación

Una vez determinado el riesgo, tipo, causa y consecuencia se debe diligenciar si efectivamente ha sido materializado, para ello se utiliza los siguientes formatos:

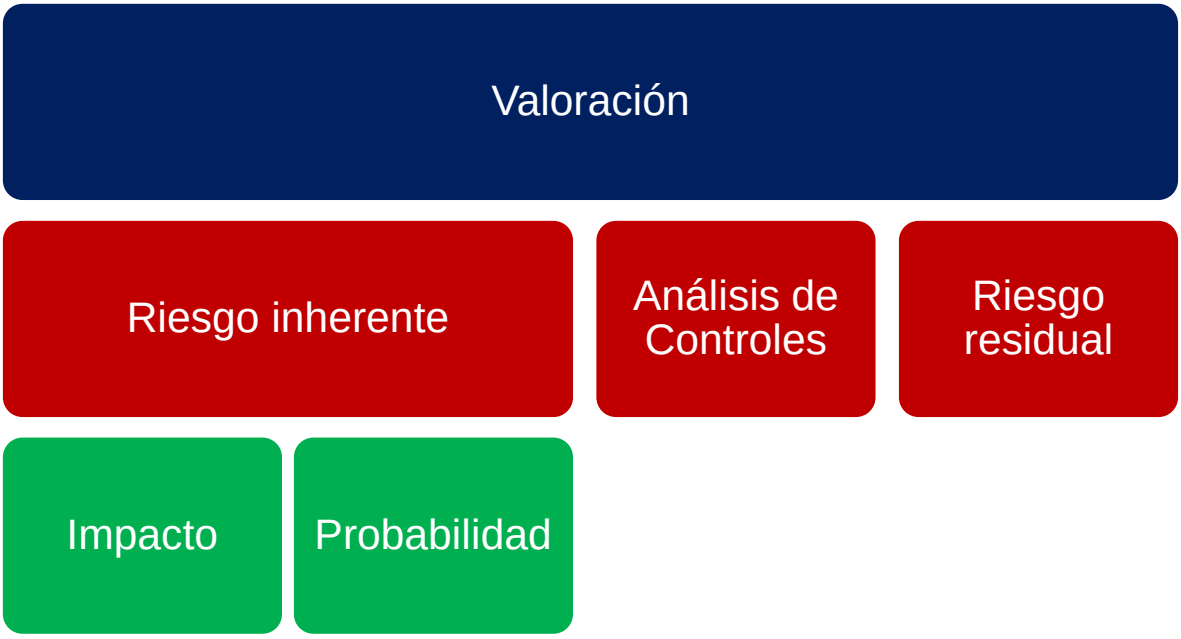
Elementos del Riesgo de gestión y corrupción: Riesgo, Tipo, Causa y Consecuencia

Elementos del Riesgo de seguridad digital: Activo, Riesgo, Tipo, Amenaza, Causa (vulnerabilidad) y Consecuencia.

2. ETAPA DE VALORACIÓN

En la valoración de los riesgos se determina el impacto y la probabilidad de ocurrencia de un evento adverso, obteniendo como resultado el riesgo inherente, al cual se le evalúan los controles aplicados y su efectividad, dando como resultado final el riesgo residual.

Ilustración 6. Etapa de Valoración.



2.1. IMPACTO

Consecuencia generada por la materialización del riesgo, se califica conforme a la afectación del riesgo.

Elementos para la determinación de consecuencias e impacto.

Consecuencia
Se enuncia la consecuencia de mayor impacto de la valoración de las afectaciones
Hechos o acontecimiento resultado de la materialización del riesgo que impactan los objetivos, metas y quehacer de la institución, están asociados a:
La estrategia
Los procedimientos y operación
Al presupuesto
La tecnología
El cumplimiento
La imagen
Los actos de corrupción
La información y seguridad digital
El medio ambiente
Los procesos académicos

Fuente: Construcción propia adaptada de la Guía para la Administración del Riesgo y el diseño de controles en entidades públicas. DAFP V: 5 diciembre 2020.

2.1.1. Situaciones que afectan el análisis del impacto:

- El riesgo de seguridad digital se determina con base en la amenaza, no en la vulnerabilidad.
- Es catastrófico cuando el riesgo ocasiona lesiones físicas o pérdidas humanas.
- Rangos de calificación de impacto:

Tabla 9. Calificación del Impacto.

Impacto	Riesgo de Gestión	Riesgo de Corrupción	Nivel
Insignificante	1-12	No aplica	1
Menor	13-24	No aplica	3
Moderado	25-36	1-15	5
Mayor	37-48	16-30	10
Catastrófico	49-60	30-60	20

Fuente: Construcción propia adaptada de la Guía para la Administración del Riesgo y el diseño de controles en entidades públicas. DAFP V: 5 diciembre 2020.

2.1.2. Impacto en los riesgos de cumplimiento asociados a la contratación

Tabla 11. Calificación del Impacto en la contratación.

Calificación	Afectación				
	Insignificante	Menor	Moderado	Mayor	Catastrófico
Ejecución	Obstruye mínimamente la ejecución del contrato.	Dificulta la ejecución del contrato de manera baja.	Afecta la ejecución del contrato sin alterar el beneficio de las partes.	Afecta la ejecución del contrato alterando el beneficio de las partes.	Obstruye la ejecución del contrato y afecta el objeto.
Económica	Los sobrecostos no representan más del 1% del valor del contrato	Los sobrecostos no representan más del 5% del valor del contrato	Genera un impacto sobre el valor entre el 5% y el 15%	Genera un impacto sobre el valor entre el 15% y el 30%	Genera un impacto mayor al 30% del valor del contrato.

Fuente: Construcción propia adaptada de la Guía para la Administración del Riesgo y el diseño de controles en entidades públicas. DAFP V: 5 diciembre 2020.

2.2. PROBABILIDAD

Analiza la posibilidad de ocurrencia del riesgo, expresada en términos de frecuencia o factibilidad, teniendo en cuenta su materialización y exposición.

2.2.1. Frecuencia de las actividades:

Se analiza el número de actividades típicas del proceso o dependencia y su realización. Se define a partir de:

- ✓ Planeación estratégica del proceso y dependencia (Elaboración de planes programas y proyectos).
- ✓ Actividades de seguimiento y adiestramiento de talento humano del proceso y dependencia.
- ✓ Actividades del proceso que tengan relación directa con lo jurídico y administrativo
- ✓ Planeación, ejecución y seguimiento a las actividades presupuestales, de contabilidad y cartera propias del proceso y dependencia.
- ✓ Ejecución de aplicativos y tecnología interna y externa para el funcionamiento del proceso y dependencias.

La exposición al riesgo estará asociada al número de actividades ejecutadas:

- ✓ Muy baja: la actividad que conlleva el riesgo se ejecuta como máximo 2 veces por año.
- ✓ Baja: La actividad que conlleva el riesgo se ejecuta de 3 a 23 veces por año.

- ✓ Media: La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año.
- ✓ Alta: La actividad que conlleva el riesgo se ejecuta de 501 a 5000 veces por año.
- ✓ Muy alta: La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año o no ejecuta.

Tabla 12. Nivel de probabilidad.

Frecuencia	Probabilidad de ocurrencia	Porcentaje de Probabilidad	Nivel de probabilidad
Muy baja	Rara vez	Entre 0% y el 20%	1
Baja	Improbable	Mayor al 20% e igual al 40%	2
Media	Posible	Mayor al 40% e igual al 60%	3
Alta	Probable	Mayor al 60% e igual al 80%	4
Muy alta	Casi Seguro	Mayor al 80% e igual al 100%	5

Fuente: Construcción propia adaptada de Guía para la administración del riesgo y el diseño de controles en entidades públicas. Versión 5. diciembre 2020

Teniendo en cuenta la calificación de frecuencia de realización de las actividades y las variables de actividad se obtendrá finalmente el nivel de probabilidad.

2.3. RIESGO INHERENTE

Se califica con base en la probabilidad e impacto, de acuerdo con la siguiente escala:

Tabla 13. Matriz de valoración de Riesgo.

Probabilidad	Casi Seguro	5	15	25	50	100
	Probable	4	12	20	40	80
	Posible	3	9	15	30	60
	Improbable	2	6	10	20	40
	Rara vez	1	3	5	10	20
		Insignificante	Menor	Moderado	Mayor	Catastrófico
	Impacto					

Fuente: Construcción propia adaptada de la Guía para la Administración del Riesgo y el diseño de controles en entidades públicas. DAFP V: 5 diciembre 2020.

De acuerdo con la matriz de calor que arroja el Riesgo Inherente, el nivel de riesgo y su tolerancia se clasifican en la siguiente escala:

Tabla 14. Tolerancia al Riesgo.

Nivel de Riesgo	Nivel de Tolerancia	Puntaje
Bajo	Aceptable	1-3
Medio	Moderado	4-9
Alto	Importante	10-24
Extremo	Inaceptable	25-100

Fuente: Construcción propia adaptada de la Guía para la Administración del Riesgo y el diseño de controles en entidades públicas. DAFP V: 5 diciembre 2020.

Sólo los riesgos de nivel Bajo podrán ser aceptados y no gestionados.

2.4. VALORACIÓN DE CONTROLES

Son las acciones o mecanismos establecidas a través de políticas, procedimientos u otras herramientas de gestión que contribuyen a garantizar el cumplimiento de los objetivos institucionales. Corresponde a la primera línea de defensa establecer y aplicar los controles a sus operaciones, para prevenir la materialización del riesgo, minimizarlo o detectar oportunidades para su gestión.

2.4.1. Tipos de Controles.

- ✓ Preventivos: Evitan la materialización del riesgo atacando las causas generadoras del mismo. Ejemplo: La autorización de accesos a los sistemas de información, previene que personas no autorizadas ingresen.

- ✓ Detectivos: Permiten registrar eventos ocurridos, pero no siempre evitan la materialización del riesgo, este control busca verificar, validar, cotejar, comparar o revisar. Ejemplo: Los registros de ingreso y salida a las instalaciones pueden detectar al infractor de cierta norma dentro de la institución.
- ✓ Estratégicos: Los que plasman la voluntad de la dirección universitaria y de los líderes de los procesos. Ejemplo: Políticas, Planes, programas y proyectos.
- ✓ De Gestión: Son aquellos tendientes a garantizar la ejecución de planes, políticas y objetivos institucionales, entre ellos: Indicadores de Gestión, Auditorías, Informes ejecutivos, la creación de organismos para su desarrollo y seguimiento (Comités), contratos específicos, entre otros. Ejemplo: la vinculación de gestores de calidad que verifican el cumplimiento de las orientaciones de calidad.
- ✓ Operativos: Se enfocan en documentar la ejecución de las actividades, pueden ser nacionales o internos. ejemplo: Procedimientos, manuales, guías, protocolos, instructivos, y sus herramientas de aplicación (Listas de verificación, actas, formatos) y cualquier documento que relacione funciones y responsabilidades.
- ✓ Legales y reglamentarios: Son las normas nacionales e internas que regulan la situación específicamente. Ejemplo: Leyes, Acuerdos y Resoluciones.

2.4.2. Evaluación de los Controles Existentes.

Se aplica la evaluación al riesgo inherente a partir de los controles existentes, para obtener el riesgo residual.

Elementos del control

Criterio	Aspecto a evaluar
Variables que afectan la probabilidad	
Tipo	Se determina el tipo de control que se aplica al riesgo
Control	Se describe el control evidencia de cómo se ejecuta
Responsable	Se identifica el cargo responsable de la ejecución del control
Sistema digital	El control puede estar controlado de forma manual o por sistemas digitales
Difusión del control	Forma en la que el control es comunicado a sus ejecutores
Variables que afectan el impacto	
Cumplimiento y ejecución	El control se cumple o ejecuta
Periodicidad de ejecución	Tiempo en el cual se ejecuta el control
Periodicidad de seguimiento	Tiempo en el cual se realiza el seguimiento a la ejecución del control

Fuente: Construcción propia

Con los resultados se califica el rango:

Tabla 15. Calificación de los Controles.

Calificación	Rangos	Concepto	Desplazamiento
Débil	0-60	El control no integra sus elementos para asegurar la prevención del riesgo.	0
Moderado	61-80	El control integra parcialmente sus elementos para asegurar la prevención del riesgo.	1 zona
Fuerte	81-100	El control integra sus elementos para asegurar la prevención del riesgo.	2 zonas

Fuente: Construcción propia adaptada de la Guía para la Administración del Riesgo y el diseño de controles en entidades públicas. DAFP V: 5. diciembre 2020.

2.5. RIESGO RESIDUAL

Realizado el análisis y calificación de los controles existentes al riesgo inherente, resulta el riesgo residual.

Tabla 16. Valoración del Riesgo Residual.

Probabilidad	Casi Seguro	5	15	25	50	100
	Probable	4	12	20	40	80
	Posible	3	9	15	30	60
	Improbable	2	5	10	20	40
	Rara vez	1	3	5	10	20
		Insignificante	Menor	Moderado	Mayor	Catastrófico
		Impacto				

Fuente: Construcción propia adaptada de la Guía para la Administración del Riesgo y el diseño de controles en entidades públicas. DAFP V: 5 diciembre 2020.

3. ETAPA DE TRATAMIENTO

Dependiendo del nivel de riesgo residual los líderes de procesos y subprocesos (Primera Línea de Defensa) determinarán la acción de tratamiento a seguir y los nuevos controles a aplicar.

3.1. ACCIONES DE TRATAMIENTO:

Tabla 17. Acciones de tratamiento.

Acciones	Descripción	Nivel de tolerancia	Efecto
Asumir	Sólo aplica al Riesgo Bajo. No se toma ninguna acción; sin embargo puede aplicarse un control como alternativa, analizando su relación costo beneficio.	Aceptable	Riesgo Residual permanece y no se gestiona.
Evitar	Se abandonan los procedimientos generadores del riesgo, como alternativa excepcional.	Moderado	Riesgo desaparece.
Reducir	Se adoptan nuevos controles o revalúan los existentes.	Aceptable, Moderado, Importante, Inaceptable.	El riesgo disminuye en cuanto a probabilidad o impacto
Compartir	Transfiere el riesgo a terceros a través de contrato.	Importante Inaceptable	No se transfiere responsabilidad, reduce sus consecuencias.

Fuente: Construcción propia adaptada de la Guía para la Administración del Riesgo y el diseño de controles en entidades públicas. DAFP V: 5 diciembre 2020.

3.2. DISEÑO DE CONTROLES PARA REDUCIR EL RIESGO

Los nuevos controles para el Riesgo Residual se definirán teniendo en cuenta:

- Para cada causa se asigna un control.
- Un control efectivo puede mitigar varias causas, caso en el cual se asociará individualmente a cada causa especifica.
- La responsabilidad del control se asigna a un cargo en particular, no a dependencias, procesos, grupos o personas.
- Los controles se evalúan de manera permanente.
- Una vez determinados se repite el ciclo de valoración de controles.

Además de los elementos del control, el diseño de controles considerará lo siguiente:

Ilustración 8. Diseño de los controles.

Responsables

Es el ejecutor del control con autoridad, competencia y conocimiento del proceso. Sus atribuciones deben ser adecuadamente segregadas o redistribuidas.

Período de ejecución

Generalmente la aplicación del control debe aplicarse con periodicidad específica (diario, mensual, trimestral, anual). El ejecutor evaluará si la periodicidad ayuda a prevenir o detectar el riesgo oportunamente. Cuando no sea posible determinar la periodicidad, se indicará su aplicación cada vez que se desarrolle la actividad.

Evidencia de la ejecución

El control debe dejar registro de ejecución y facilitar su revisión por un tercero y la verificación de su evaluación.

Fuente: Construcción propia adaptada de la Guía para la Administración del Riesgo y el diseño de controles en entidades públicas. DAFP V: 5 diciembre 2020.

4. ETAPA MONITOREO Y EVALUACIÓN

El monitoreo y evaluación se desarrolla a partir del siguiente esquema de asignación de roles y responsabilidades:

Tabla 18. Monitoreo y Evaluación por líneas de Defensa

Línea Estratégica – Dirección Universitaria y Comité Institucional de Gestión y Desempeño
❖ Monitorea y revisa el cumplimiento de los objetivos institucionales gestionando los riesgos desde: ❖ Los cambios en el direccionamiento estratégico y el efecto sobre la gestión del riesgo. ❖ Los informes periódicos de seguimiento y de auditoría a la gestión del riesgo. ❖ La revisión al cumplimiento a los objetivos institucionales y de los procesos. ❖ La valoración a la efectividad del Plan de Contingencia.
Primera línea de Defensa – Líderes de procesos, subprocesos, programas y proyectos de la entidad.
❖ Monitorea y revisa el cumplimiento de los objetivos institucionales gestionando los riesgos desde: ❖ La articulación de los cambios del Direccionamiento Estratégico con la gestión del riesgo. ❖ Orientación de la mejora a la gestión del riego a partir de los informes periódicos de seguimiento y de auditoría a la gestión del riesgo. ❖ Auto valoración de sus procedimientos de supervisión, la revisión del diseño y ejecución de los controles. ❖ Verificación a la documentación y actualización de los controles en los procedimientos.

❖ El reporte a la OPDI, sobre la materialización de los riesgos y sus causas. ❖ La revisión del Plan de Contingencia.
Segunda línea de Defensa – Oficina de Planeación y Desarrollo Institucional, supervisores e interventores de contratos o proyectos, coordinadores de otros sistemas de gestión de la entidad, comités de riesgos (donde existan), comités de contratación, entre otros.
❖ Monitorea y revisa el cumplimiento de los objetivos institucionales gestionando los riesgos desde: ❖ El apoyo a la actualización de los mapas de riesgos, a partir de los cambios en el direccionamiento estratégico. ❖ Las recomendaciones a la correcta definición y articulación de los objetivos de los procesos y subprocesos con los objetivos institucionales. ❖ El apoyo a la formulación y fortalecimiento de los controles. ❖ El seguimiento a la documentación y actualización de los controles. ❖ El apoyo a la revisión y actualización del Plan de Contingencia.
Tercera Línea de Defensa – Oficina de Control Interno
❖ Monitorea y revisa de manera independiente y objetiva el cumplimiento de los objetivos institucionales, aportando a la gestión del riesgo, desde: ❖ La revisión de los cambios en el direccionamiento estratégico o entorno, que permita actualizar los mapas de riesgos de los procesos y/o subprocesos. ❖ La revisión a la correcta identificación de los riesgos. ❖ La revisión a la pertinencia y efectividad de los controles, y recomendar su fortalecimiento. ❖ Los requerimientos a la actualización de los mapas de riesgos por procesos, con base en los resultados de auditorías o autoevaluaciones. ❖ La verificación y actualización de la efectividad de los controles. ❖ La comunicación de los procesos sobre los resultados de la evaluación a los riesgos.

Fuente: Construcción propia adaptada de la Guía para la Administración del Riesgo y el diseño de controles en entidades públicas. DAFP V: 5 diciembre 2020.

4.1. RESPONSABILIDADES EN LOS. ACTIVOS DE SEGURIDAD DE LA INFORMACIÓN

La Resolución R-785 de 2015 adoptó la política del Sistema de Gestión de Seguridad de la Información de la Universidad del Cauca.

Respecto de las responsabilidades, corresponde a la Primera Línea de Defensa con la orientación del responsable de seguridad digital designado; lo siguiente:

- ❖ Identificar los Activos: El líder de cada proceso identificará cuántos y cuáles están bajo la responsabilidad del proceso.
- ❖ Definir los Activos: Listarlos con la identificación del responsable y clasificarlos conforme a Información física y digital, software, hardware, Componentes de Red, etc.
- ❖ Clasificar la información: Según los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.

- ❖ Determinar la criticidad del activo: Según la confidencialidad, integridad, y disponibilidad (alto, medio y bajo).
- ❖ Informar al responsable de seguridad digital sobre el acontecimiento de alguna contingencia sobre los activos.

4.2. MATRIZ DE MONITOREO Y SEGUIMIENTO

El seguimiento se adelantará con periodicidad cuatrimestral diligenciando por lo menos los siguientes ítems de la siguiente matriz:

Matriz de monitoreo y seguimiento.

Proceso Estratégico
Oficina de Planeación y Desarrollo Institucional
Matriz de Monitoreo a Riesgos Universidad del Cauca

Código:PE-GE-2.4-OD-4					Versión: 2			Fecha de Vigencia: 21-10-2021												
	Identificación					Valoración			Tratamiento											
No	Proceso	Tipo de Riesgo	Riesgo	Causa/Vulnerabilidad	Consecuencias	Nivel de Riesgo Inherente	Control Existentes	Nivel de Riesgo Residual	Tratamiento	Control	Responsables	Periodicidad	Tipo de Contol	Evidencia	Fecha de monitoreo	Actividades realizadas	Descripción de las actividades realizadas	Evidencias	Observaciones	

La presente metodología se desarrollará conforme a los formatos Herramientas para la construcción – MARUC. Código: PV-GC-2.6-OD-03, Matriz de Riesgos; Código: PV-GC2.6-FOR-9, Mapa de Riesgos Institucional: PE-GE- 2.4-OD-3 y Monitoreo y Seguimiento a Riesgos Institucionales, PE-GE-2.4-OD-4.

4.2.1. Materialización del Riesgo

A la inminente materialización del riesgo, el responsable del proceso procede a:

- ❖ Verificar la existencia del control del riesgo en el Plan de Contingencia y aplicarlo.
- ❖ Identificar el responsable del control y su competencia para ejecutarlo.
- ❖ Comunicar al competente cuando el responsable directo del control no cuenta con las facultades necesarias, a fin de que direccione las medidas para tratar el riesgo.
- ❖ Enterar de la situación la OPDI para que direccione medidas para tratar el riesgo.
- ❖ Instruir al ejecutor del control para aplicar el plan de contingencia.
- ❖ Monitorear el comportamiento del riesgo y dejar los registros.
- ❖ Informar a las instancias administrativas y disciplinarias, cuando se trate de riesgos de corrupción.
- ❖ Cuando un proceso determine alta certeza de materialización de un evento que afecte los objetivos Institucionales y no esté considerado en el mapa de riesgos, debe informarse a la OPDI, para:
- ❖ Actualizar el mapa de riesgos y el plan de contingencia.
- ❖ Definir el control e iniciar su ejecución.

- El responsable del proceso monitoreará la efectividad del control y reportará la evolución a la OPDI (Segunda Línea de defensa) y ésta a la Dirección (Línea estratégica) cuando se estime conveniente a su solución.

4.2.2. Indicadores

El responsable del Proceso, con los ejecutores del procedimiento, define los indicadores de eficacia y efectividad como herramienta de medición a la aplicación de las acciones de tratamiento. Serán referentes los siguientes:

- En Riesgo de Gestión y Corrupción.

Eficacia: Índice de cumplimiento actividades= (N° de actividades cumplidas / N° de actividades programadas) x 100.

Efectividad: Plan de manejo de riesgos= ((N° de casos de favorecimiento presentados periodo actual – N° de casos de favorecimiento presentados periodo anterior) / N° de casos de favorecimiento presentados periodo anterior) x 100.

- En Riesgo de Seguridad Digital:

Eficacia: Porcentaje de controles implementados = (Controles implementados / N° controles definidos) x 100.

Efectividad: N° Riesgos materializados de confidencialidad = (N° de incidentes que afectaron la confidencialidad de algún activo del proceso) o Variación de incidentes de confidencialidad (para entidades con mediciones anteriores) = ((N° de Incidentes de Confidencialidad Periodo Actual – N° de Incidentes de Confidencialidad Periodo Previo) / Incidentes de Confidencialidad Periodo Previo) * 100%.

5. COMUNICACIÓN Y DIVULGACIÓN

La gestión del riesgo se divulgará y comunicará para la construcción participativa permitiendo:

- Establecer correctamente el contexto para los procesos.
- Considerar las necesidades de los usuarios.
- Garantizar la correcta identificación de los riesgos.
- Articular las áreas de mayor experticia en el análisis de los riesgos.
- Considerar las distintas perspectivas del riesgo.
- Ubicar la gestión del riesgo dentro del proceso de planeación estratégica.
- Fomentar la administración del riesgo como una actividad inherente al proceso de planeación estratégica.

- Corresponde a la OPDI difundir y asesorar la metodología y acompañar en la definición e implementación de planes de tratamiento.

6. HERRAMIENTA PARA LA ADMINISTRACIÓN DEL RIESGO

Los conceptos técnicos determinados en la MARUC, se aplicarán a través de la herramienta elaborada en formato Excel, la cual integra los formatos para agotar el ciclo de Administración del Riesgo: identificación, valoración, tratamiento y monitoreo y evaluación.

Esta herramienta es parte integral de la MARUC y se incluye como anexo único.

III. BIBLIOGRAFÍA

- ✓ “Guía Administración del Riesgo” octubre de 2018 Departamento Administrativo de la Función Pública.
- ✓ “Guía Administración del Riesgo y diseño de controles” diciembre de 2020 Departamento Administrativo de la Función Pública.
- ✓ “Guía de auditoría interna basada en riesgos para entidades públicas” julio de 2020 Departamento Administrativo de la Función Pública.
- ✓ NTC ISO 31000:2018 ICONTEC https://www.invias.gov.co/index.php/archivo-y-documentos/cnsc/proyectos-de-resolucion/7554-propuesta-politica-de-administracion-de-riesgo-2018/file.
- ✓ https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf.
- ✓ https://www.mintic.gov.co/portal/604/articles-14481_recurso_1.pdf (infraestructura física). El estudiante como cliente: riesgo para la calidad de la educación superior en Colombia.
- ✓ ftp://backups.senado.gov.co/meci/Manual_MECI/Unidad_2/A_control%20estrategico/A_1_ambiente%20control/A_1_3_estilo%20direccion/A_1_3_lectura.htm (Estilo de dirección).
- ✓ http://gaia.gobiernobogota.gov.co/sites/default/files/sig/manuales/ple-pin-m001_0.pdf guía.
- ✓ https://www.mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf
- ✓ Guía para la Gestión y Clasificación de Activos de Información.
- ✓ https://www.pmg-ssi.com/2017/02/realizar-inventario-activos-de-informacion/datos básicos de un activo de información.
- ✓ https://www.colciencias.gov.co/sites/default/files/upload/paginas/g104m02-manual-de-activos-de_-informacion.
- ✓ https://www.defensajuridica.gov.co/servicios-al-ciudadano/ley_transparencia/Documents/guia_inventario_activos_clasificacion_publicacion_de_informacion_130916.pdf.