UNIVERSIDAD DE CUNDINAMARCA

MANUAL - LINEAMIENTO DE ADMINISTRACIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

FUSAGASUGÁ
2024

TABLA DE CONTENIDO

1. INTRODUCCIÓN 4
2. OBJETIVOS 5
2.1 OBJETIVO GENERAL 5
2.2 OBJETIVOS ESPECÍFICOS 5
3. ALCANCE 6
4. DEFINICIONES 6
5. MARCO LEGAL Y NORMATIVO DE SEGURIDAD DE LA INFORMACIÓN 9
6. MARCO CONCEPTUAL 9
6.1 ESTABLECIMIENTO DEL CONTEXTO 10
6.2 IDENTIFICACIÓN, ANÁLISIS Y VALORACIÓN DEL RIESGO 10
6.3 TRATAMIENTO DE RIESGOS 11
6.4 MONITOREO Y REVISIÓN 11
6.5 COMUNICACIÓN Y CONSULTA 11
6.6 REGISTRO E INFORME 11
7. METODOLOGÍA PARA LA GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN 12
7.1 LINEAMIENTO DE ADMINISTRACIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN 12
7.2 ESTABLECIMIENTO DEL CONTEXTO 12
7.2.1 Contexto Externo 12
7.2.2 Contexto interno 13
7.2.3 Gestión de activos de información 13
7.3 EVALUACIÓN DEL RIESGO 14
7.3.1 Identificación del riesgo 14
7.3.2 Análisis de riesgos 21
7.3.3 Valoración del riesgo 24
7.3.4. Tratamiento de los Riesgos Residuales 28
7.4 MONITOREO Y REVISIÓN 30
7.5 COMUNICACIÓN Y CONSULTA 32
7.6 REGISTRO E INFORME 32

8. BIBLIOGRAFÍA Y WEB GRAFÍA. 33

1. INTRODUCCIÓN

El presente documento hace parte de las estrategias para la implementación del Modelo de Seguridad y Privacidad de la Información – MSPI de Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC, donde uno de sus principales lineamientos es la identificación, valoración y tratamiento de los riesgos asociados tanto al Sistema de Gestión de Seguridad de la Información – SGSI, enmarcado en el cumplimiento de los estipulado en el numeral 6 de la norma ISO IEC 27001:2022.

Por tanto, la respectiva gestión de riesgos se realiza siguiendo lo expuesto en la Guía para la administración del riesgo y el diseño de controles en entidades públicas emitida por el Departamento Administrativo de la Función Pública - DAFP y su respectivo Anexo 4 - Lineamientos para le gestión de riesgos de seguridad digital en entidades públicas generada por el MinTIC.

Por lo anterior en este documento se establecen los lineamientos para la identificación, análisis, valoración, tratamiento, monitoreo y seguimiento de los riesgos que pudieran afectar la misión, el cumplimiento de los objetivos estratégicos y la gestión de los procesos, proyectos y planes institucionales.

2. OBJETIVOS

2.1 OBJETIVO GENERAL

Definir los lineamientos y metodología para identificar, analizar, valorar y tratar los riesgos asociados a la seguridad de la información de la Universidad de Cundinamarca, que puedan afectar el logro de sus objetivos estratégicos y operacionales, generando posibles sanciones, pérdidas económicas y/o reputacionales por medio del compromiso y/o afectación de sus activos de la información.

2.2 OBJETIVOS ESPECÍFICOS

- Establecer el contexto interno y externo de la Universidad de Cundinamarca, en el que se puede dar la materialización de riesgos de seguridad de la información.

- Identificar las vulnerabilidades y amenazas a las que están expuestos los activos de información, que puedan causar alguna afectación en la confidencialidad, integridad y disponibilidad de estos.

- Definir los criterios para realizar la valoración de los riesgos de seguridad de la información según su probabilidad de ocurrencia y el impacto en los objetivos estratégicos y operacionales de la institución.

- Determinar los elementos requeridos para monitorear y dar seguimiento a los riesgos de seguridad de la información y a los planes de tratamiento según sea el caso.

- Identificar los riesgos de seguridad de la información en la Universidad de Cundinamarca, a partir de los activos de información con criticidad alta y muy alta.

3. ALCANCE

La administración de riesgos de seguridad de la información es responsabilidad de todos los procesos de la Universidad de Cundinamarca (Estratégicos, Misionales, de Apoyo y de Seguimiento), representada principalmente por los propietarios de activos de información o líderes y/o gestores responsables de proceso. Esta metodología da cumplimiento a los requerimientos legales, normativos, reglamentarios, contractuales y propios de la Universidad de Cundinamarca.

4. DEFINICIONES

Activo de Información: Cualquier información o elemento relacionado con el tratamiento de esta que tenga valor para la organización.[1]

Amenaza: Causa potencial de un incidente no deseado, que puede causar daños a un sistema u organización.[2]

Análisis del riesgo: Proceso para comprender la naturaleza del riesgo y para determinar el nivel de riesgo. (ISO 27000 Términos y definiciones).

Apetito al riesgo: Nivel de riesgo a nivel gerencial, que la Compañía está dispuesta a aceptar en seguimiento al valor y logro de los objetivos.

Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.[3]

Consecuencia: Resultado de un evento que afecta los objetivos.[4]

Control: Medida que mantiene o modifica al riesgo (ISO 31000, Términos y definiciones). Las políticas, procedimientos, prácticas, dispositivos y estructuras organizacionales que están diseñados para brindar una confianza razonable de que se alcanzarán los objetivos del negocio y que se evitarán, o bien, detectarán y corregirán los eventos no deseados.

Disponibilidad: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.[5]

Evaluación de riesgo: Proceso usado para identificar y evaluar riesgos y sus posibles efectos. La evaluación de riesgo incluye la evaluación de las actividades

[1] https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en
[2] Ibidem
[3] Ibidem
[4] Ibidem
[5] Ibidem

mínimas y necesarias de una organización para continuar las operaciones del negocio. (ISO 27000 Términos y definiciones).

Evento: Ocurrencia o cambio de un conjunto particular de circunstancias:

- Un evento puede tener una o más ocurrencias y puede tener varias causas y varias consecuencias.
- U
- n evento también puede ser algo previsto que no llega a ocurrir, o algo no previsto que ocurre.
- Un evento puede ser una fuente de riesgo. (ISO 31000, Términos y definiciones).

Fuente o factor de riesgo: Elemento que solo o en combinación con otros, tiene el potencial de generar el riesgo. (ISO 31000, Términos y definiciones).

Gestión del Riesgo: Actividades coordinadas para dirigir y controlar la Organización con relación al riesgo (ISO 31000, Términos y definiciones).

Identificación del Riesgo: Proceso de encontrar, reconocer y describir los riesgos. [6]

Impacto: Cambio adverso en el nivel de los objetivos del negocio logrados. (ISO 27005, Términos y definiciones).

Integridad: Propiedad de la información relativa a su exactitud y completitud.[7]

Líder del Proceso: Responsable de la administración de un proceso; es decir, de su planeación, organización, dirección y control.

Matrices de Riesgo: Bases de datos que contienen toda la información necesaria para identificar una clase de riesgo en particular, incluyendo sus características, los controles y planes de contingencia establecidos, y los responsables de estos. Estas Matrices también contienen una calificación o rating para cada riesgo.

Parte Interesada: Persona u organización que puede afectar, verse afectada, o percibirse como afectada por una decisión o actividad (ISO 31000, Términos y definiciones).

Perfil de Riesgo: Resultado consolidado de la medición de los riesgos a los que se ve expuesta una entidad.

Probabilidad: Posibilidad que suceda un evento determinado. La posibilidad de que ocurra algo, ya sea definido, medido o determinado objetiva o subjetiva, cualitativa o

[6] https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en
[7] Ibidem

cuantitativamente, y descrito usando términos generales o matemáticamente (como una probabilidad o una frecuencia en un período de tiempo determinado).

Proceso: Conjunto interrelacionado de actividades para la transformación de elementos de entrada en productos o servicios, para satisfacer una necesidad, tanto interna como externa.

Propietario del riesgo: Persona con la responsabilidad de rendir cuentas y la autoridad para gestionar un riesgo (ISO 31000, Términos y definiciones).

Riesgo en la seguridad de la información: Potencial de que una amenaza determinada explote las vulnerabilidades de los activos o grupos de activos causando así daño a la organización [8]

Riesgo inherente: Nivel de riesgo propio de la actividad, sin tener en cuenta el efecto.

Riesgo residual: Riesgo remanente después del tratamiento del riesgo (ISO 31000, Términos y definiciones).

SGSI: Sistema de Gestión de Seguridad de la Información.

Tratamiento del riesgo: Proceso de modificar el riesgo (ISO 27000 Términos y definiciones). Puede incluir:

- Evitar el riesgo al decidir no comenzar o continuar con la actividad que genera el riesgo.
- Tomar o aumentar el riesgo para perseguir una oportunidad.
- Remover el riesgo.
- Cambiar la probabilidad.
- Cambiar las consecuencias.
- Compartir el riesgo con otra parte o partes (incluidos los contratos y la financiación del riesgo).
- Retener el riesgo por elección informada.

Los tratamientos de riesgo que tratan con consecuencias negativas a veces se denominan “mitigación de riesgo”, “eliminación de riesgo”, “prevención de riesgo” y “reducción de riesgo”. El tratamiento del riesgo puede crear nuevos riesgos o modificar los riesgos existentes. [9]

Valoración del riesgo: Proceso de comparación de los resultados del análisis de riesgo con los criterios de riesgo para determinar si el riesgo y / o su magnitud es aceptable o tolerable (ISO 27000 Términos y definiciones).

[8] https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en
[9] Ibidem

Vulnerabilidad: Una deficiencia en el diseño, la implementación, la operación o los controles internos en un proceso que podría explotarse para violar la seguridad del sistema.[10]

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas.[11]

- Una consecuencia puede ser cierta o incierta y puede tener efectos directos o indirectos positivos o negativos en los objetivos.
- Las consecuencias se pueden expresar de manera cualitativa o cuantitativa.
- Cualquier consecuencia puede incrementarse por efectos en cascada y acumulativos.

5. MARCO LEGAL Y NORMATIVO DE SEGURIDAD DE LA INFORMACIÓN

- Ley 1712 de 2014 “Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.” (Artículo 13,20)
- Resolución 092 de 2023 “Por la cual se adopta el Sistema de Seguridad de la Información – SGSI y se establecen Lineamientos, Objetivos y Alcance en la Universidad de Cundinamarca”.
- Resolución 027 de 2018 “Por la cual se establecen los roles y responsabilidades de los Sistemas de Gestión de la Universidad de Cundinamarca".
- Resolución 088 “Por la cual se establece el sistema de aseguramiento de la calidad de la universidad de Cundinamarca”.
- Norma Técnica NTC-ISO IEC 27001:2022 del Sistema de Gestión de Seguridad de la Información
- Guía para la Administración del Riesgo el diseño de controles en entidades públicas emitida por el Departamento Administrativo de la Función Pública (DAFP)
- Guía No.7 “Gestión de Riesgos” generadas por el MinTic.

6. MARCO CONCEPTUAL

La metodología desarrollada para la gestión de riesgos de seguridad de la información está alineada con las necesidades propias del negocio y las buenas prácticas presentes en el marco normativo de la Guía No 7 - Gestión de Riesgos emitida por el MinTIC basada en la ISO/IEC 27005 Gestión de riesgos para la seguridad de la información y la Guía

[10] https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en
[11] Ibidem

para la administración del riesgo y el diseño de controles en entidades públicas emitida por el Departamento Administrativo de la Función Pública – DAFP, tal como se muestra en la siguiente figura:

Ilustración 1 Proceso de gestión del riesgo de seguridad de la información tomado de la Guía para la Administración del Riesgo y el diseño de controles en entidades públicas

.

6.1 ESTABLECIMIENTO DEL CONTEXTO

El objetivo de esta etapa es determinar qué factores internos y externos pueden impactar a la institución, qué requiere protección y de acuerdo con los recursos actuales cómo podría darse esa protección, determinando los alcances y limitaciones existentes. La identificación correcta del contexto organizacional es la base para identificar los riesgos y facilitar el análisis y la gestión de estos.

6.2 IDENTIFICACIÓN, ANÁLISIS Y VALORACIÓN DEL RIESGO

Determinar que podría suceder que cause una perdida potencial, y llegar a comprender el cómo, donde, y por qué podría ocurrir está perdida, esto consiste en priorizar los riesgos identificados, clasificándolos de acuerdo con su potencial de pérdida y su probabilidad de ocurrencia, a través de una medición cuantitativa o cualitativa de los efectos probables asociados a los riesgos. Lo anterior suministra

datos fundamentales para la toma de acciones en el tratamiento de estos y diseñar las estrategias sobre las cuales la organización podrá optar por evitar, prevenir, controlar, retener o transferir los riesgos.

6.3 TRATAMIENTO DE RIESGOS

Identificar los controles existentes e implementados para mitigar los riesgos evaluados, utilizando como referencia el Anexo A de la norma ISO 27001:2022. Estos controles pueden incluir, pero no se limitan a, controles organizacionales, de personas, tecnológicos y físicos. Luego de elegir cuáles controles son los más adecuados para tener un nivel de riesgo aceptable para el o los procesos incluidos en el alcance del SGSI, se debe diseñar un plan de tratamiento de riesgos incluyendo los de Seguridad de la información, en el cual se defina qué tratamiento se dará a los riesgos qué acciones se implementarán, quienes serán los responsables de esta implementación. Este plan debe plantear claramente cada acción, etapa y procedimientos que se ejecutarán para poder ser monitoreado y lograr el seguimiento a la ejecución de este.

6.4 MONITOREO Y REVISIÓN

Se refiere al planteamiento de una serie de alternativas de acuerdo con el tipo de estrategia seleccionada, que involucra acciones a seguir, responsables de su ejecución y seguimientos a la efectividad de estas.

6.5 COMUNICACIÓN Y CONSULTA

Como elemento transversal del sistema de gestión del riesgo, contempla el desarrollo de un plan de comunicaciones permanente a través del proceso Seguridad de la Información, dirigido a todas las partes interesadas e involucradas dentro del sistema ya sean internas o externas. Incluyen un diálogo bilateral que permita centrar esfuerzos hacia la mejora de este. Al alcanzar los acuerdos sobre cómo administrar los riesgos, considerando su naturaleza, probabilidad, consecuencias, tratamiento y aceptación, el siguiente paso es comunicar el riesgo a los dueños de procesos.

6.6 REGISTRO E INFORME

Se documenta e informa el proceso de gestión de riesgos de seguridad de la información y sus resultados, esto tiene como finalidad proporcionar información para la toma de decisiones, mejorar las actividades de gestión del riesgo y promover la interacción con las partes interesadas.

7. METODOLOGÍA PARA LA GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

7.1 LINEAMIENTO DE ADMINISTRACIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

La Universidad de Cundinamarca asume el compromiso de administrar los riesgos de seguridad de la información que puedan afectar de manera negativa el alcance de los objetivos estratégicos y objetivos de procesos de la institución; del mismo modo busca forjar una institución más proactiva que reactiva, previniendo y reduciendo los efectos no deseados promoviendo la mejora continua, propendiendo una organización basada en la acción preventiva automática enfocada en la administración del riesgo, con control en todos los niveles de la institución, brindando seguridad razonable destinando los esfuerzos necesarios para administrar los riesgos que se puedan presentar en la Universidad de Cundinamarca.

Así mismo desde el Sistema de Gestión de Seguridad de la Información - SGSI actualmente se cuenta con el procedimiento ESG-SSI-P12 - GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN, en el que se describen las actividades a seguir en relación con las fases descritas en la ilustración 1 del numeral 6, que inicia con el contexto organizacional y termina con la documentación del proceso de la gestión de riesgos, este proceso se realiza de manera periódica anualmente o cuando surgen cambios en el contexto de la institución (cambios en los procesos, activos de información o materialización de incidentes).

7.2 ESTABLECIMIENTO DEL CONTEXTO

Por medio del análisis del contexto, la Universidad de Cundinamarca articula sus objetivos, define los parámetros externos e internos que se van a considerar al gestionar el riesgo, establece el alcance y los criterios del riesgo para el resto del proceso.

7.2.1 Contexto Externo

Es el ambiente externo en el cual la Universidad de Cundinamarca busca alcanzar sus objetivos, realizar este proceso es importante ya que se garantiza que los objetivos y las preocupaciones de las partes involucradas externas se tomen en consideración al desarrollar los criterios del riesgo. Es importante resaltar que el contexto involucra toda la Universidad de Cundinamarca.

Algunos de los factores externos que están relacionados con el contexto institucional son:

- Legales
- Financieros
- Tecnológicos

- Políticos
- Medioambientales
- Socioculturales
- Relaciones con otras entidades
- Clientes
- Proveedores
- Económico

7.2.2 Contexto interno

Es el ambiente interno en el cual la Universidad de Cundinamarca busca alcanzar sus objetivos, así mismo, es todo aquello que pueda tener influencia en la forma en que la Universidad de Cundinamarca gestionará el riesgo. Algunos de los factores internos tenidos en cuenta para establecer el contexto organizacional son:

- Conocer la estrategia de la organización (misión, visión y objetivos estratégicos)
- Identificar las características de los procesos del negocio (caracterización de procesos)
- Estructura organizacional
- Infraestructura
- Recursos humanos
- Tecnología
- Recursos financieros
- Sistemas de información
- Procesos y procedimientos
- Administración
- Cultura organizacional
- Relaciones contractuales

7.2.3 Gestión de activos de información

La realización de un inventario y clasificación de activos hace parte de la debida diligencia que a nivel estratégico se ha definido en el Modelo de Seguridad y Privacidad de la Información MSPI con respecto a la seguridad de los activos de información de los procesos de una entidad, y cuyo objetivo es dar cumplimiento a los numerales 5.9 Inventarios de Activos de información y otros activos asociados, 5.12 Clasificación de la Información y 5.13 Etiquetado de la Información de la NTC ISO/IEC 27001:2022 y su Anexo A, lo anterior se realiza de acuerdo con el procedimiento ESG-SSI-P01 “Gestión de Activos de información” y demás documentos que lo complementen.

- Inventario y propiedad de activos: todos los activos deben estar claramente identificados y la entidad debe elaborar y mantener un inventario de los mismos con su respectivo propietario.
- Clasificación de la información: La información se debe clasificar según las necesidades de Seguridad de la información de la organización en función de la confidencialidad, integridad, disponibilidad y los requisitos pertinentes de las partes interesadas.
- Etiquetado: Debe elaborarse y aplicarse un conjunto adecuados de procedimientos para el etiquetado de la información de conformidad con el plan de clasificación de la información adoptado por la institución.

7.3 EVALUACIÓN DEL RIESGO

La evaluación del riesgo es el proceso completo de identificación, análisis y valoración de riesgos, este proceso proporciona una mejor comprensión de los riesgos que podrían afectar el logro de los objetivos de la Universidad de Cundinamarca.

7.3.1 Identificación del riesgo

En esta etapa del proceso se descubren, reconocen y caracterizan los riesgos actuales o potenciales que puedan afectar el logro de los objetivos de la Universidad de Cundinamarca, independientemente si están o no controlados.

Los riesgos de los procesos se encuentran entre otros a través de datos históricos, el análisis del proceso y sus respectivos procedimientos, auditorías y reuniones de expertos en las que participan los directores y el Oficial o responsable seguridad de la información.

Pueden utilizarse diferentes fuentes de información de la Universidad de Cundinamarca, tales como registros históricos, experiencias significativas, registro de eventos o debilidades de seguridad de la información o eventos de seguridad asociadas a las bases de datos, análisis de vulnerabilidades, pruebas de Ethical Hacking e ingeniería social, informes de auditorías previas, indicadores, la técnica utilizada y las fuentes consultadas dependerá de las necesidades y naturaleza del análisis a realizar.

Nota: Los líderes del proceso y su equipo de trabajo son los responsables de identificar los riesgos de su proceso.

Para complementar lo anteriormente descrito, a continuación, se realiza una descripción general de posibles riesgos asociados a la Universidad de Cundinamarca.

7.3.1.1 Riesgos de seguridad de la información

La identificación de los riesgos de seguridad de la información asociados a los procesos de la Universidad de Cundinamarca, se desarrollan de manera coordinada entre los propietarios de activos de información o líderes de proceso a través de reuniones programadas entre las partes y es necesario contar con el consolidado institucional de activos de información. Este insumo se obtiene como resultado de las actividades del procedimiento **ESG-SSI-P01– GESTIÓN DE ACTIVOS DE LA INFORMACIÓN** del proceso Gestión Sistemas Integrados, debidamente formalizado en el Sistema de Gestión de Calidad - SGC de la Universidad de Cundinamarca.

Los riesgos de seguridad de la información componen una lista de situaciones que pueden tener una afectación o impacto en los tres pilares de la seguridad de la información (confidencialidad, integridad y disponibilidad). En la identificación de estos riesgos debe tener en cuenta el activo afectado por la materialización del riesgo, entendiéndose por activo de información todo aquello que contiene información que es valiosa para la organización y por lo tanto debe protegerse adecuadamente.

Además, se muestra el identificador y la descripción asignado a cada riesgo, como se establece en el formato **ESG-SSI-F039 - MATRIZ DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN.**

IDENTIFICADOR	RIESGO
R1	Perdida de la confidencialidad
R2	Perdida de la integridad
R3	Perdida de la disponibilidad

La respectiva descripción del riesgo se realizará en la matriz de acuerdo a los tres pilares de seguridad (Confidencialidad, Integridad y Disponibilidad) los cuales se asociarán con los diferentes tipos de activos de información identificados en la vigencia, a continuación, se describen algunos ejemplos de riesgos asociados a los activos de información:

CÓDIGO DEL RIESGO	TIPO DE ACTIVO	RIESGO
R1-HW	HARDWARE	Perdida de Confidencialidad
R2-SW	SOFTWARE	Perdida de Integridad
R3-SE	SERVICIOS	Perdida de Disponibilidad
R4-IN	INFORMACIÓN	Perdida de Disponibilidad
R5-IL	INSTALACIONES	Riesgos Legales

Tabla 1 Ejemplos de Riesgos de Seguridad de la Información.

7.3.1.2 Posibles vulnerabilidades de los activos de información

Luego de realizar la identificación de los riesgos de seguridad de la información se deben identificas las vulnerabilidades que son inherentes para los activos de información, estas pueden estar en las siguientes áreas:

- Organización.
- Procesos y procedimientos.
- Rutinas de gestión.
- Personal.
- Ambiente físico.
- Configuración del sistema de información.
- Hardware, software y equipos de comunicaciones.
- Dependencia de partes externas.

A continuación, se describen las posibles vulnerabilidades presentes en lo activos de información sin limitarse a estas y se define una tipificación de mediante el identificador **V1, V2, V3...,** las cual se deberán tener en cuenta en el diligenciamiento del formato Matriz de Riesgos en Seguridad de la Información.

IDENTIFICADOR	VULNERABILIDAD
V1	Mantenimiento insuficiente y/o fuera de la planeación
V2	Falta de programa para disposición final de RAEE's
V3	Daños ocasionados por humedad, polvo o suciedad
V4	Susceptibilidad a las variaciones de voltaje
V5	Almacenamiento sin protección
V6	Falta de cuidado en la disposición final
V7	Copia no controlada
V8	Ausencia o insuficiencia de pruebas de software
V9	Defectos bien conocidos en el software
V10	Ausencia de "terminación de sesión" cuando se abandona la estación de trabajo
V11	Disposición o reutilización de los medios de almacenamiento sin borrado adecuado
V12	Ausencias de pistas de auditoria
V13	Asignación errada de los derechos de acceso
V14	En términos de tiempo utilización de los datos errados en los programas de aplicación
V15	Interfaz de usuario compleja
V16	Ausencia de documentación
V17	Configuración incorrecta de parámetros
V18	Fecha y horas incorrectas
V19	Ausencia de mecanismos de identificación y autenticación, como la autenticación de usuario
V20	Tablas de contraseñas sin protección

IDENTIFICADOR	VULNERABILIDAD
V21	Gestión deficiente de las contraseñas
V22	Habilitación de servicios innecesarios
V23	Software nuevo o inmaduro
V24	Ausencia de requerimientos funcionales de seguridad para los desarrollos internos o contratados externamente
V25	Ausencia de control de cambios eficaz
V26	Descarga y uso no controlado de software
V27	Ausencia de copias de respaldo
V28	Ausencia de protección física de la edificación, puertas y ventanas
V29	Documento controlado por el Sistema de Gestión de la Calidad
V30	Ausencia de un eficiente control de cambio en la accesibilidad de los servicios
V31	Asignación errada al acceso de servicios.
V32	Líneas de comunicación y navegación sin protección
V33	Arquitectura insegura de red.
V34	Acceso a servicios en conexión de red pública sin protección
V35	Ausencia de políticas sobre el uso del correo electrónico
V36	Ausencia de procedimientos para el manejo de información clasificada
V37	Ausencia de autorización de los recursos de procesamiento de información
V38	Ausencia de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales
V39	Ausencia del personal
V40	Procedimientos inadecuados de contratación
V41	Entrenamiento insuficiente en seguridad
V42	Uso incorrecto de software y hardware
V43	Falta de conciencia acerca de la seguridad
V44	Ausencia de mecanismos para la gestión de vulnerabilidades técnicas en la plataforma tecnológica.
V45	Trabajo no supervisado del personal externo o de limpieza
V46	Ausencia de políticas para el uso correcto de los medios de telecomunicaciones y mensajería
V47	Ausencia de procedimiento formal para el registro y retiro de usuarios
V48	Ausencia de asignación adecuada de roles y responsabilidades en seguridad de la información
V49	Ausencia de responsabilidad en seguridad de la información en la descripción de los cargos
V50	Ausencia de los procesos disciplinarios definidos en caso de incidentes de seguridad de la información

IDENTIFICADOR	VULNERABILIDAD
V51	Ausencia de revisiones regulares por parte de la gerencia
V52	Ausencia de procedimientos para la presentación de informes sobre las debilidades en la seguridad en los procesos internos y a los entes de control
V53	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos
V54	Ausencia periódica de esquemas de reemplazo
V55	Ausencia de una gestión de la configuración eficiente
V56	Susceptibilidad a las variaciones de temperatura
V57	Ausencia de identificación y autentificación de emisor y receptor
V58	Transferencia de contraseñas en claro
V59	Ubicación en un área susceptible de inundación
V60	Red energética inestable
V61	Ausencia de proceso formal para la revisión (supervisión) de los derechos de acceso
V62	Ausencia o insuficiencia de disposiciones (con respecto a la seguridad) en los contratos con los clientes y/o terceras partes
V63	Ausencia de auditorías (supervisiones) regulares
V64	Ausencia de procedimientos de identificación y valoración de riesgos
V65	Ausencia de reportes de fallas en los registros de administradores y operadores
V66	Respuesta inadecuada de mantenimiento del servicio
V67	Ausencia de acuerdos de nivel de servicio, o insuficiencia en los mismos.
V68	Ausencia de procedimiento de control de cambios
V69	Ausencia de procedimiento formal para la autorización de la información disponible al público
V70	Ausencia de planes de continuidad
V71	Ausencia de registros en las bitácoras (logs) de administrador y operario.
V72	Ausencia o insuficiencia en las disposiciones (con respecto a la
V73	seguridad de la información) en los contratos con los empleados
V74	Ausencia de política formal sobre la utilización de computadores portátiles
V75	Ausencia de control de los activos que se encuentran fuera de las instalaciones
V76	Ausencia o insuficiencia de política sobre limpieza de escritorio y de pantalla

IDENTIFICADOR	VULNERABILIDAD
V77	Ausencia de revisiones regulares por parte de la Alta Dirección
V78	Ausencia de procedimientos para la presentación de informes sobre las debilidades en la seguridad
V79	Fallas en el procedimiento de gestión de acceso a usuarios de servicios informáticos
V80	Errores o abuso de los privilegios en la administración de las bases de datos por parte del operador tecnológico
V81	Debilidades en la implementación del procedimiento interno de Gestión de Incidentes de Seguridad de la información

Tabla 2 Posibles vulnerabilidades de seguridad de la información.

7.3.1.3 Amenazas de seguridad

Luego de identificar las vulnerabilidades que son inherentes para los activos de información, se deben establecer las amenazas que se pueden aprovechar de las vulnerabilidades y materializar el riesgo. Las amenazas pueden ser de origen natural o humano y podrían ser accidentales o deliberadas es recomendable identificar todos los orígenes de las amenazas accidentales como deliberadas. A continuación, se describen las posibles amenazas y se define la tipificación mediante el identificador **A1, A2, A3...,** las cual se deberán tener en cuenta en el diligenciamiento del formato Matriz de Riesgos en Seguridad de la Información.

IDENTIFICADOR	AMENAZA
A1	Incumplimiento en el mantenimiento correctivo y/o preventivo
A2	Hurto a medios o documentos
A3	Incumplimiento de la ley 1672 de 2013
A4	Daños físicos (fuego, daño por agua, contaminación, accidente importante, destrucción del equipo o los medios, polvo, corrosión, congelamiento) que puede causar pérdida de información
A5	Pérdida del suministro de energía
A6	Abuso de los derechos de acceso y privilegios
A7	Corrupción de datos
A8	Error de uso
A9	Falsificación de derechos
A10	Procesamiento ilegal de datos
A11	Mal funcionamiento del software
A12	Manipulación con software
A13	Uso no autorizado del equipo
A14	Espionaje remoto
A15	Uso de software falsificado o copiado
A16	Incumplimiento en la disponibilidad del personal

IDENTIFICADOR	AMENAZA
A17	Destrucción de equipos y medios
A18	Negación de acciones.
A19	Hurto de equipos
A20	Ciberataques
A21	Eventos naturales (fenómenos climáticos, fenómenos sísmicos, fenómenos volcánicos, fenómenos meteorológicos, inundación)
A22	Orden público
A23	Pérdida de servicios esenciales (falla en el sistema de suministro de agua o de aire acondicionado, pérdida de suministro de energía, falla en el equipo de telecomunicaciones)
A24	Sanciones o llamados de atención de entes de vigilancia y control
A25	Saturación del sistema de información
A26	Datos provenientes de fuentes no confiables
A27	Falla del equipo
A28	Procesamiento ilegal de datos
A29	Realizar transferencias internacionales a países que no ofrezcan un nivel de protección adecuado.
A30	Fuga de información
A31	Errores en los procesos de recopilación y captura de información
A32	Modificación no autorizada de datos

Tabla 3 Posibles amenazas de seguridad de la información.

Adicionalmente para realizar una identificación de vulnerabilidades y amenazas de acuerdo con el contexto actual es necesario conocer las amenazas más comunes en la industria de seguridad.

7.3.1.4 Consecuencias del riesgo

Ahora se debe identificar la magnitud de los efectos que puede ocasionar la materialización del riesgo, se determina considerando el grado de daño en los activos de información o los cambios en los objetivos definidos por la organización. A continuación, se describen las posibles consecuencias y tipificación de mediante el identificador **Q1, Q2, Q3...,** las cual se deberán tener en cuenta en el diligenciamiento del formato Matriz de Riesgos en Seguridad de la Información.

IDENTIFICADOR	CONSECUENCIA
Q1	Pérdida de la continuidad del negocio, servicios afectados para los usuarios internos y externos. Afectación a toda la entidad

IDENTIFICADOR	CONSECUENCIA
Q2	Divulgación, alteración o pérdida de información confidencial
Q3	Retraso o deficiencia en procesos estratégicos y misionales
Q4	Baja calidad o interrupción en los servicios estratégicos y misionales
Q5	Sanciones legales o multas por parte de entes de control.
Q6	Pérdidas económicas

Tabla 4 Posibles consecuencias en seguridad de la información.

7.3.1.5 Dueño del riesgo

En esta parte se debe identificar dueño del riesgo, este tiene la responsabilidad y autoridad para gestionar un riesgo.

7.3.2 Análisis de riesgos

En este punto se busca establecer la probabilidad de ocurrencia del riesgo y su impacto, teniendo en cuenta las vulnerabilidades, amenazas y consecuencias identificadas. Para ello basado en la guía del DAFP, se define los criterios o niveles de probabilidad de ocurrencia e impacto, con el fin de que el dueño del riesgo analice y determine estos dos aspectos.

7.3.2.1 Determinar la probabilidad de ocurrencia del riesgo

Es la posibilidad de ocurrencia del riesgo, esta puede ser medida en términos de frecuencia, si el riesgo se ha materializado o no, en un periodo establecido y la factibilidad teniendo en cuenta la presencia de factores externos e internos que puedan propiciar el riesgo, aunque este no se haya materializado. La probabilidad se modela como una tasa anual de ocurrencia, para esto de acuerdo con lo definido por el DAFP se definen los siguientes criterios que permiten identificar y definir el nivel de probabilidad de forma objetiva y real, como se muestra en la siguiente tabla.

	Frecuencia de la Actividad	Probabilidad
Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año	20%
Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año	40%
Media	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año	60%
Alta	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5000 veces por año	80%
Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año	100%

Tabla 5 Criterios para definir el nivel de probabilidad - Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas. Versión 6. Dirección de Gestión y Desempeño Institucional. Departamento Administrativo de la Función Pública.

7.3.2.2 Determinar el nivel de Impacto del riesgo

El impacto se considera como el conjunto de posibles efectos negativos que puede ocasionar el riesgo en caso de materializarse, como variables principales se definen afectaciones económicas y/o reputacionales como lo señala la guía del DAFP. Es necesario tener en cuenta que cuando se presenten ambos impactos para un riesgo, tanto económico como reputación, con diferentes niveles se debe tomar el nivel más alto, así, por ejemplo: para un riesgo identificado se define un impacto económico en nivel insignificante e impacto reputación en nivel moderado, se tomará el más alto, en este caso sería el nivel moderado.

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

Tabla 6 Criterios para definir el nivel de impacto - Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas. Versión 6. Dirección de Gestión y Desempeño Institucional. Departamento Administrativo de la Función Pública.

7.3.2.3 Determinar el Riesgo Inherente

Luego de determinar la probabilidad de ocurrencia e impacto del riesgo, se determina el nivel de severidad a través de la combinación entre la probabilidad y el impacto (*Riesgo Inherente=Probabilidad*Impacto).* Se definen 4 zonas de severidad en la matriz de calor, la cual será representada en una Matriz de 5x5 con la que se establecerá el Perfil del Riesgo Inherente, como se ilustra a continuación:

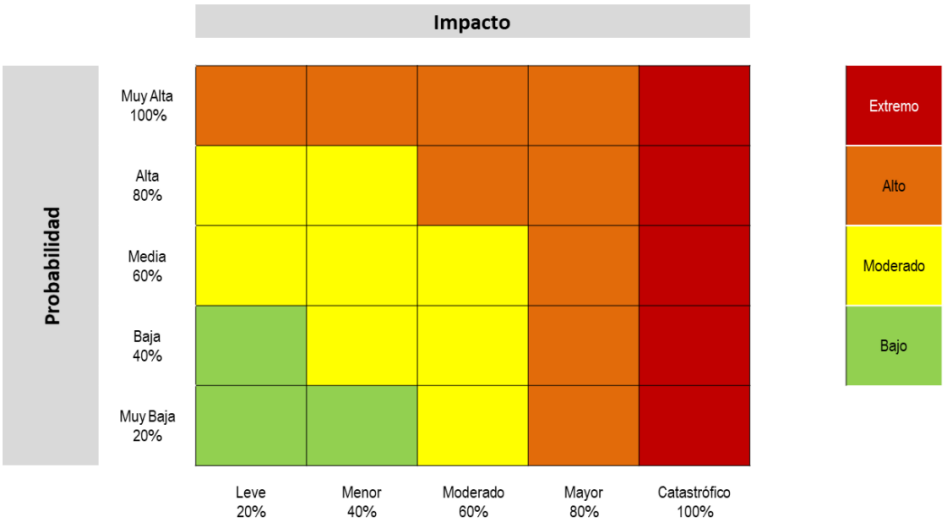


Tabla 7 Matriz de calor (niveles de severidad del riesgo) - Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas. Versión 6. Dirección de Gestión y Desempeño Institucional. Departamento Administrativo de la Función Pública

De acuerdo con lo anterior, se construye una matriz de 5x5 con probabilidad e impacto categorizados de 1 al 5, como se evidencia a continuación:

			Impacto				
			Leve	Menor	Moderado	Mayor	Catastrófico
			1	2	3	4	5
Probabilidad	Muy Alta	5	5	10	15	20	25
	Alta	4	4	8	12	16	20
	Media	3	3	6	9	12	15
	Baja	2	2	4	6	8	10
	Muy baja	1	1	2	3	4	5

Tabla 8 Mapa de calor de niveles de impacto del riesgo.

7.3.3 Valoración del riesgo

En este punto se busca identificar los controles y evaluar los controles de seguridad existentes en la institución, los cuales permiten mitigar la probabilidad de ocurrencia e impacto asociados a las amenazas y vulnerabilidades que hacen que el riesgo se pueda materializar.

7.3.3.1 Identificación de controles

Para garantizar el tratamiento de los riesgos evaluados, se deben identificar los controles y/o medidas de seguridad existentes que permitan disminuir los valores de exposición del riesgo inherente. Para esta identificación, se debe tener en cuenta:

a) Descripción del control: Descripción del control implementado
b) Evidencia (soporte): Evidencia que respalde el control implementado
c) Responsabilidad del control: Descripción del cargo, área o proceso que implementa el control
d) Frecuencia del control: Frecuencia con la que el control es implementado, esta puede ser:
   - Diario
   - Semanal
   - Mensual
   - Trimestral
   - Semestral
   - Anual
   - Por demanda

Nota: Los controles a colocar para los riesgos de seguridad de la información (SGSI) deben ser coherentes con los establecidos en el Anexo A de la Norma ISO 27001.

7.3.3.2 Análisis y Evaluación del control

Para el análisis y evaluación de los controles se deben tener en cuenta los siguientes atributos:

ATRIBUTOS	CATEGORÍA	DESCRIPCIÓN	PESO POR CATEGORÍA
Tipo de control	Preventivo	Se toma esta opción cuando el riesgo no se ha materializado. (ataca probabilidad)	3
	Detectivo	Identifican los eventos en el momento en que se presentan. (ataca probabilidad)	2

ATRIBUTOS	CATEGORÍA	DESCRIPCIÓN	PESO POR CATEGORÍA
	Correctivo	Se toma esta opción cuando el riesgo se ha materializado. (ataca impacto)	1
Documentación	Formal	Existe información documentada formalmente aprobada, socializada y publicada.	3
	Informal	Existe información documentada aprobada. Sin embargo, no ha sido socializado ni publicado.	2
	Ninguno	No existe información documentada.	1
Aplicación	Siempre	El control siempre es aplicado por el responsable.	3
	Aleatorio	El control es aplicado aleatoriamente por el responsable.	2
	A discreción	El control es aplicado a discreción del responsable.	1
Naturaleza del control	Automático	Es realizado por un sistema informático sin la intervención humana	3
	Semiautomático	Es realizado por humanos y con la intervención de un sistema informático	2
	Manual	Es realizado por humanos sin la intervención de un sistema informático	1
Efectividad La efectividad depende del resultado de la sumatoria de la evaluación de los controles.	Alta	El control se ejecuta según las condiciones definidas de manera consistente por parte del responsable.	3
	Media	El control se ejecuta cumpliendo parcialmente las condiciones, se	2

ATRIBUTOS	CATEGORÍA	DESCRIPCIÓN	PESO POR CATEGORÍA
		ejecuta algunas veces por parte del responsable.	
	Baja	El control no se ejecuta adecuadamente por parte del responsable.	1

Tabla 9 Atributos de para el diseño del control - Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas. Versión 6. Dirección de Gestión y Desempeño Institucional. Departamento Administrativo de la Función Pública.

7.3.3.2.1 Valor del control

Es el promedio de los valores resultado de Tipo de control, Naturaleza del control, documentación, aplicación, naturaleza de control y efectividad del control.

7.3.3.2.2 Valor consolidado de los controles

Es el promedio de calificación de los controles aplicados para mitigar el riesgo.

7.3.3.2.3 Mitigación del Control

Se calcula dependiendo el tipo de control, los controles preventivos mitigan la probabilidad, los controles detectivos y correctivos mitigan el impacto, según esta definición en las columnas de probabilidad e impacto se indica (SI O NO) referente al control que mitiga. Luego dependiendo la mitigación del control, se calcula una probabilidad e impacto total, este valor total se da con impacto o probabilidad inherentes, menos el valor consolidado del control.

7.3.3.2.4 Riesgo residual

Es el resultado de aplicar la efectividad de los controles al riesgo inherente, de acuerdo con la mitigación de la probabilidad e impacto, el riesgo residual se calcula automáticamente de acuerdo con la mitigación anteriormente mencionada.

7.3.3.3 Apetito del riesgo

Teniendo en cuenta el nivel de riesgo residual calculado y la tolerancia al riesgo aprobada por la alta dirección, se deben tomar acciones según lo definido a continuación:

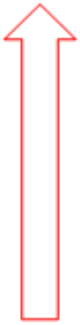
NIVEL DE RIESGO	DESCRIPCIÓN	TOLERANCIA	
EXTREMO	En ninguna circunstancia se deberá mantener un riesgo con este efecto en el logro de los objetivos, por lo cual requerirá atención inmediata y de alta prioridad para buscar disminuir su severidad. Éstos deberán ser reportados a la alta dirección de forma inmediata y la definición del plan de acción, no debe ser superior a 1 mes. Cualquier excepción, deberá ser aprobada por alta dirección.		NO TOLERABLE
ALTO	Requiere que se ejecuten acciones prioritarias a corto plazo, debido al alto efecto que tendrían sobre el logro de los objetivos. Estos deberán ser reportados a la alta dirección de forma inmediata y la definición del plan de acción, no debe ser superior a 2 meses. Cualquier excepción, deberá ser aprobada por la alta dirección.		
MODERADO	Se administra con procedimientos rutinarios, conservando y/o mejorando los controles documentados para mantener el nivel de riesgo.		TOLERABLE
BAJO	Se administra con procedimientos rutinarios, conservando los controles documentados para mantener el nivel de riesgo.		

Tabla 10 Identificación de niveles de riesgo tolerables y no tolerables

A continuación, se muestra gráficamente los riesgos cuyo nivel de riesgo residual no es tolerable para Universidad de Cundinamarca, corresponden a las celdas en color naranja y rojo y los cuales requieren la formulación de planes de tratamiento:

			Impacto				
			Leve	Menor	Moderado	Mayor	Catastrófico
			1	2	3	4	5
Probabilidad	Muy Alta	5	5	10	15	20	25
	Alta	4			12	16	20
	Media	3				12	15
	Baja	2				8	10

	Muy baja	**1**				**4**	**5**

Tabla 11 Niveles de impacto del riesgo no tolerables

7.3.3.4 Aceptación de riesgos residuales

- Los riesgos residuales que están dentro de la zona tolerable deben tener la aceptación del riesgo residual por parte del dueño del riesgo, esta aceptación debe quedar documentada, formalizada y puede ser consultada en el repositorio del SGSI.
- Las aceptaciones de riesgos de seguridad de la información se deben reportar al líder de seguridad de la información para su seguimiento correspondiente.
- La aceptación de riesgos residuales no tolerables con ausencia de planes de tratamiento debe realizarse por parte de la alta dirección.
- A nivel general las aceptaciones de riesgo de seguridad de la información deben ser revisadas por la alta dirección como mínimo una vez al año.

7.3.4. Tratamiento de los Riesgos Residuales

El propietario del riesgo, una vez conocido el riesgo residual, debe aceptar el nivel de riesgo y decidir la opción de tratamiento para cada uno de los riesgos a los que está expuesta la Universidad de Cundinamarca. Esta decisión puede ser aceptar, reducir o evitar el riesgo. Dependiendo de la decisión tomada, se determinará la necesidad de definir planes de acción dentro del correspondiente mapa de riesgos. En la siguiente figura se muestran las tres opciones mencionadas y su relación con la necesidad de definir planes de acción.

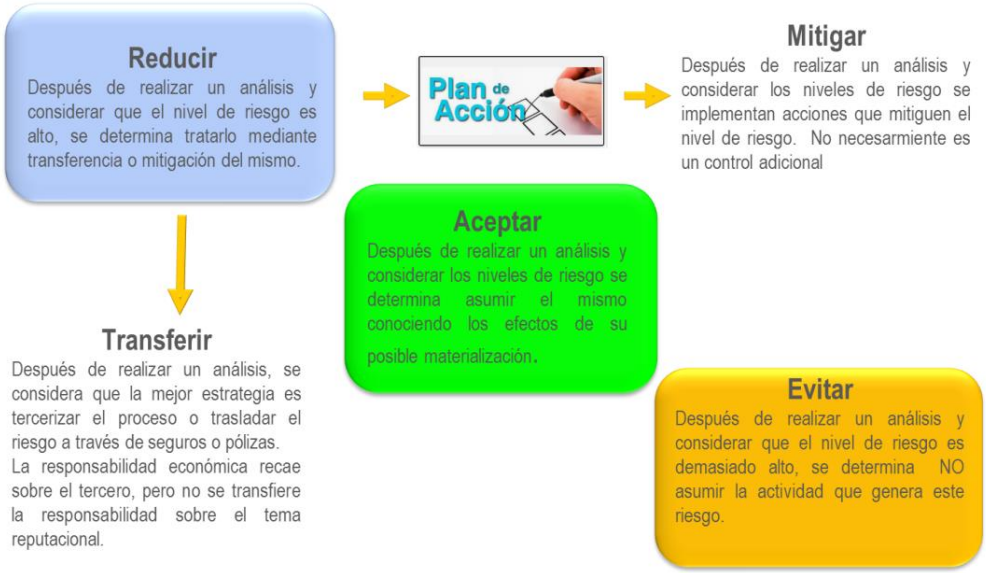


Ilustración 2 Estrategias para combatir el riesgo tomado de la Guía para la Administración del Riesgo y el diseño de controles en entidades públicas

OPCIONES DE TRATAMIENTO DE RIESGO		
Reducir	Mitigar	Esta estrategia busca, bien reducir la probabilidad de ocurrencia de un riesgo, bien reducir sus consecuencias, o lograr ambos objetivos a la vez. Un riesgo puede mitigarse a través de controles de gestión y procedimientos encaminados a reducir la frecuencia o el impacto generado. Se requiere plan de tratamiento.
	Transferir	Hace referencia a buscar respaldo y compartir con otro parte del riesgo. Se trasladan las posibles pérdidas por eventos de riesgo a otras empresas a través de arreglos contractuales, tercerización de procesos y seguros, con el fin de compartir el riesgo. Se requiere plan de tratamiento.
Evitar		Determinación de la Universidad de Cundinamarca de finalizar o dar por terminada la actividad o procedimiento que exponía a la compañía a cierto riesgo que ya no se está dispuesto a tener. Se requiere plan de tratamiento.
Aceptar		Cuando se acepta un riesgo se asumen las consecuencias en el momento que se presenten. **Nota:** No puede haber aceptación de riesgos sobre situaciones que conlleven a incumplimientos normativos.

Tabla 12 Opciones de Tratamiento de Riesgos

Para efectos del mapa de riesgos, cuando se define la opción de reducir, se requerirá la definición de un plan de acción que especifique, como mínimo lo siguiente:

- Acciones generales y/o controles a implementar.
- Responsable (cargo o rol).
- Fecha de inicio de acciones o controles a implementar.
- Fecha fin de acciones o controles a implementar.
- Estado (programado, ejecutado, pendiente y en ejecución)
- Porcentaje de Avance
- Producto de la actividad ejecutada

El diseño, desarrollo y aprobación del plan de acción o de tratamiento debe ser realizada por parte del dueño del riesgo para cada uno de los riesgos seleccionados. Además, los dueños de riesgos deben monitorear la ejecución del plan de tratamiento, como parte del desarrollo de su trabajo con relación a la gestión de riesgos, organiza los planes de tratamiento y a medida que se presentan las fechas de cumplimiento de los compromisos revisa su ejecución y si los responsables de la ejecución comunican que existen inconvenientes para su cumplimiento lo notifica al líder de seguridad de la información, con quien se revisa y se actualizan las fechas. En caso de ser

necesario, el dueño del riesgo obtendrá la aprobación de nuevas fechas con la Alta dirección.

Nota: El Sistema de Gestión de Seguridad de la Información en conjunto con el líder del proceso realiza la revisión de los planes posterior a su ejecución. La matriz de riesgo es revisada anualmente o cuando surjan cambios en el contexto organizacional por el Sistema de Gestión de Seguridad de la Información en conjunto con el líder del proceso.

7.4 MONITOREO Y REVISIÓN

Está etapa está alineada con la dimensión de “Control Interno”, del Modelo Integrado de Planeación y Gestión – MIPG, el monitoreo y revisión tiene como propósito valorar la efectividad de los controles establecidos por la institución, el nivel de ejecución de los planes de acción o tratamiento de los riesgos que permiten asegurar los resultados de la gestión, así como detectar las desviaciones y tendencias para generar recomendaciones sobre el mejoramiento de los procesos, y determinar si existen cambios en el contexto interno o externo, incluyendo los cambios en los criterios de riesgo y en el propio riesgo.

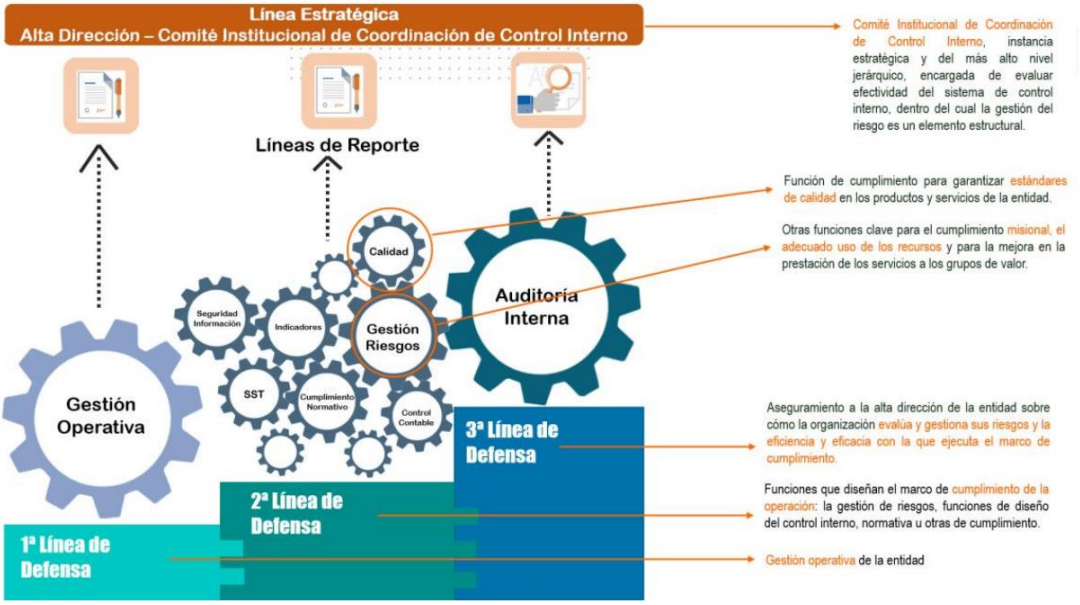


Ilustración 3 Operatividad Esquema de líneas de defensa tomado de la Guía para la Administración del Riesgo y el diseño de controles en entidades públicas

Por lo anterior en la Universidad de Cundinamarca, esta etapa opera de la siguiente manera:

LÍNEA	RESPONSABLE	RESPONSABILIDADES
LÍNEA ESTRATÉGICA	Alta Dirección Comisión de Desempeño Comisión de Gestión	• Define el marco general para la gestión del riesgo y el control, mediante el establecimiento de la política de administración del riesgo.
1ERA LÍNEA DE DEFENSA (gestión operacional)	A cargo de los líderes de los procesos, programas y proyectos de la institución.	• Desarrollar e implementar procesos de control y gestión de riesgos a través de su identificación, análisis, valoración, monitoreo y acciones de mejora. • Diseñar, implementar y monitorear los controles y gestionar de manera directa en el día a día los riesgos de la institución. • Orientar el desarrollo e implementación de políticas y procedimientos internos y asegurar que sean compatibles con las metas y objetivos de la institución y emprender las acciones de mejoramiento para su logro. • Cada líder de proceso debe mantener la traza o documentación respectiva de todas las actividades realizadas que garanticen de forma razonable que dichos riesgos no se materializarán y por ende que los objetivos del proceso se cumplan.
2DA LÍNEA DE DEFENSA	Director(a) de planeación, supervisores e interventores de contratos o proyectos, coordinadores de otros sistemas de gestión de la institución, comités de riesgos (donde existan), comités de contratación, entre otros.	• Asegura que los controles y los procesos de gestión de riesgos implementados por la primera línea de defensa, estén diseñados apropiadamente y funcionen como se pretende. • Monitorear la gestión de riesgo y control ejecutada por la primera línea de defensa, complementando su trabajo, así como, el aseguramiento sobre el diseño apropiado de los controles.
3RA LÍNEA DE DEFENSA	Dirección de Control Interno, auditoría	• A través de sus procesos de seguimiento y evaluación,

	interna o quien haga sus veces.	especialmente a través de la auditoría interna deben establecer la efectividad de los controles para evitar la materialización de riesgos.

Tabla 13 Responsabilidad frente a la gestión del riesgo de las líneas de defensa tomado de la Guía para la Administración del Riesgo y el diseño de controles en entidades públicas.

7.5 COMUNICACIÓN Y CONSULTA

La comunicación y la consulta debe darse en todas las etapas de la gestión de riesgos de seguridad de la información en el marco de un proceso participativo que involucre actores internos y externos de la institución, permitiendo ayudar a establecer el contexto estratégico, ayudar a determinar que los riesgos estén correctamente identificados, reunir diferentes áreas de experticias para el análisis de los riesgos y fomentar la gestión de riesgos en la Universidad de Cundinamarca.

Así mismo los resultados de esta gestión quedan documentados en la matriz de riesgos, la cual se comunicará oportunamente a los dueños de riesgo y alta dirección a través de correo electrónico, adicionalmente cada matriz podrá ser consultada en el repositorio de cada proceso disponible en el Modelo de Operación Digital de la Universidad de Cundinamarca. Adicionalmente desde el Sistema de Gestión de Seguridad de la Información – SGSI se custodiarán las últimas versiones de las matrices de riesgos y documentación complementaria que soporte para la gestión del riesgo realizada, dando cumplimiento a lo dispuesto Guía para la Administración del Riesgo y el diseño de controles en entidades públicas del DAFP y el numeral 9 de la ISO 27011:2022.

7.6 REGISTRO E INFORME

Desde el Sistema de Gestión de Seguridad de la Información – SGSI de acuerdo con lo dispuesto en el numeral 9.3 Revisión por la Dirección, los resultados de la evaluación de riesgos y estado de los planes de tratamiento de riesgos según sea el caso serán parte de las entradas para la revisión por la dirección.

8. BIBLIOGRAFÍA Y WEB GRAFÍA.

- Guía para la administración del riesgo y el diseño de controles en entidades públicas. Versión 6. Dirección de Gestión y Desempeño Institucional. Departamento Administrativo de la Función Pública.

- Guía No. 7 gestión de riesgos del Ministerios de las Tecnologías y las Comunicaciones -MINTIC.

- NTC-ISO-IEC 27005-2020 gestión de riesgos de seguridad de la información.

- NTC-ISO-IEC 27000-2018 vocabulario del sistema de gestión de seguridad de la información.

- UNE-ISO 31000-2018 gestión del riesgo.

CONTROL DE CAMBIOS				
VERSIÓN	FECHA DE APROBACIÓN			DESCRIPCIÓN DEL CAMBIO
	AAAA	MM	DD	
1	2021	05	13	Emisión del Documento
2	2021	10	13	Unificación de riesgos, vulnerabilidades, amenazas y consecuencias asociadas a protección de datos y seguridad de la información.
3	2023	03	31	Se anexa nueva terminología con relación a las vulnerabilidades, amenazas y se articula el tratamiento del control con base a la norma ISO/IEC/2001:2013.
4	2024	07	29	Se ajusta objetivo general, específicos y alcance del presente documento, se agregaron definiciones y ajusto el documento en general de acuerdo con la Guía para la Administración del Riesgo y el diseño de controles en entidades públicas Versión 6 y la Norma ISO 27001:2022. Según la resolución rectoral 074 del 22 de julio del 2024, dando cumplimiento a la ley 2345 del 2023 "chao marcas" y dando alcance a la circular 006 "Cambio de identificador visual en los documentos de gestión documental" se realiza el cambio de logo en el documento.

ELABORÓ	
NOMBRES Y APELLIDOS	CARGO
Fabián Libardo Parra Gutiérrez	Técnico
Brayan Esteban Ortegón Palomino	Técnico

REVISÓ	
NOMBRES Y APELLIDOS	CARGO
María del Pilar Delgado Rodríguez	Coordinadora del SGSI Profesional Universitario I.

APROBÓ (GESTOR RESPONSABLE DEL PROCESO)				
NOMBRES Y APELLIDOS	CARGO	FECHA		
		AAAA	MM	DD
María del Pilar Delgado Rodríguez	Coordinadora del SGSI Profesional Universitario I	2024	07	29