UNIVERSIDAD DE CUNDINAMARCA

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Elaborado por: SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

FUSAGASUGÁ
2025

TABLA DE CONTENIDO

1. INTRODUCCIÓN

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información se establece como una estrategia integral, destinada a generar acciones preventivas que mitiguen los riesgos asociados con los activos de la información de la Universidad de Cundinamarca. Este plan busca evaluar, identificar, analizar y tratar periódicamente los riesgos en cada una de sus etapas, manteniendo su valoración en un nivel residual aceptable.

Para lograr el objetivo, el plan define acciones concretas que deben tomarse para mitigar los riesgos identificados. Estas acciones están organizadas en actividades específicas, cada una con tareas claramente definidas, responsables asignados y tiempos mediante cronogramas establecidos para su ejecución. Este enfoque detallado permite monitorear y lograr el seguimiento de los riesgos por proceso y/o área a nivel institucional.

Asimismo, el plan actúa como una línea estratégica que promueve el desarrollo y fortalecimiento de una cultura organizacional, consciente del riesgo y su contexto en toda la universidad y su implicación de llegarse a materializar, por lo anterior se debe fortalecer las capacidades internas para responder adecuadamente ante incidentes relacionados con la seguridad y privacidad de la información e implementar, implantando una cultura sobre el tratamiento adecuado de los riesgos.

2. OBJETIVO GENERAL

Establecer el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, conforme a los lineamientos y directrices emitidos por los entes de control, acorde a la normatividad legal vigente, que permitan mitigar la materialización de riesgos potenciales de seguridad y privacidad de la información.

2.1 OBJETIVOS ESPECÍFICOS

- Identificar y actualizar los riesgos de seguridad y privacidad de la información de los procesos de la Universidad de Cundinamarca conforme a los controles de la norma ISO 27001:2022.

- Analizar y determinar los riesgos de seguridad y privacidad de la información, con base en la identificación, análisis, evaluación y valoración de estos, de acuerdo con lo establecido en el ESG-SSI-P12 – "*GESTION DE RIESGOS DE SEGURIDAD DE LA INFORMACION*".

- Evaluar los riesgos residuales de Seguridad y Privacidad de la Información, protegiendo y preservando la integridad, confidencialidad, disponibilidad de la información

- Tratar los riesgos de Seguridad y Privacidad de la información, con el fin de mantener los riesgos en una zona tolerable.

- Monitorear y revisar el desarrollo de los planes de tratamiento definidos.

- Fortalecer y promover una cultura referente a la gestión de riesgos de Seguridad y Privacidad de la información, con el fin de aplicar medidas correctivas en caso de la materialización de un riesgo.

3. ALCANCE

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información aplica a todos los procesos y/o áreas de la Universidad de Cundinamarca que registraron los activos de la información y cuentan con matriz de riesgos. Se enfoca en gestionar y tratar todos los riesgos de seguridad y privacidad de la información, en especial los que se encuentran en la zona de riesgo Moderado, Alto o Extremo, los cuales superan el nivel de riesgo aceptable, con la finalidad de generar mecanismos de prevención y mitigación de los mismos, fortalecer la toma de decisiones y la prevención frente a la materialización de incidentes de seguridad y privacidad de la información que puedan afectar el logro de los objetivos institucionales.

Un adecuado tratamiento y gestión de los riesgos debe contar con la participación de todas las áreas de la Universidad de Cundinamarca, con el fin de conocer, apropiar e implementar las directrices y lineamientos definidos y realizar el seguimiento o monitoreo correspondiente de acuerdo con lo establecido en el ESG-SSI-P12 – “GESTION DE RIESGOS DE SEGURIDAD DE LA INFORMACION”.

4. DEFINICIONES

AMENAZA: es un ente o escenario interno o externo que puede hacer uso de una vulnerabilidad para generar un perjuicio o impacto negativo en la institución (materializar el riesgo). [1]

CONTROL O MEDIDA: Medida que permite reducir o mitigar un riesgo. [2]

IMPACTO: consecuencias que puede ocasionar a la organización la materialización del riesgo. [3]

MAPA DE RIESGOS: documento con la información resultante de la gestión del riesgo.

PROBABILIDAD: se entiende la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. [4]

RIESGO: efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales. [5]

RIESGO DE SEGURIDAD DE LA INFORMACIÓN: posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000). [6]

RIESGO INHERENTE: nivel de incertidumbre propio de cada actividad, sin la ejecución de ningún control.[7]

RIESGO RESIDUAL: nivel restante de riesgo después del tratamiento del riesgo.[8]

TRATAMIENTO: Cualquier operación o conjunto de operaciones sobre el tratamiento de un riesgo.[9]

VULNERABILIDAD: es una falencia o debilidad que puede estar presente en la tecnología, las personas o en las políticas y procedimientos. [10]

[1] Guía para la administración del riesgo y el diseño de controles en entidades públicas - DAFP (2024)
[2] ISO/IEC 27000
[3] Guía para la administración del riesgo y el diseño de controles en entidades públicas - DAFP (2024)
[4] ISO/IEC 27000
[5] Guía para la administración del riesgo y el diseño de controles en entidades públicas - DAFP (2024)
[6] ISO/IEC 27000
[7] ISO/IEC 27000
[8] Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información V.6 – MINTIC
[9] Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información V.6 – MINTIC
[10] ISO/IEC 27000

5. LINEAMIENTO DE ADMINISTRACIÓN DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El objetivo del lineamiento es establecer los parámetros necesarios para una adecuada gestión y tratamiento de los Riesgos de Seguridad y Privacidad de la Información, procurando que no se materialicen, atendiendo los lineamientos establecidos en la Guía para la administración del riesgo y el diseño de controles en entidades públicas del DAFP, orientando a la toma de decisiones oportunas y minimizando efectos adversos al interior de la Institución, con el fin de asegurar el cumplimiento objetivos misionales y la mejora continua.

El tratamiento de riesgos es la respuesta establecida por la primera línea de defensa, es decir, el líder o responsable del proceso junto con su equipo de trabajo y el Sistema de Gestión de Seguridad de la Información - SGSI para la mitigación de los diferentes riesgos.

El tratamiento o respuesta dada al riesgo, se enmarca en las siguientes categorías:

Aceptar el riesgo: No se adopta ninguna medida que afecte la probabilidad o el impacto del riesgo. La aceptación del riesgo puede ser una opción viable en la institución, para los riesgos bajos, pero también pueden existir escenarios de riesgos a los que no se les puedan aplicar controles de la Norma ISO 27001:2022 y, por ende, se acepta el riesgo. En ambos escenarios debe existir un seguimiento continuo del riesgo.

Reducir el riesgo: Se adoptan medidas para reducir la probabilidad o el impacto del riesgo, o ambos; por lo general conlleva a la implementación de controles. Deben seleccionarse controles apropiados y con una adecuada segregación de funciones, de manera que el tratamiento al riesgo adoptado logre la reducción prevista sobre este.

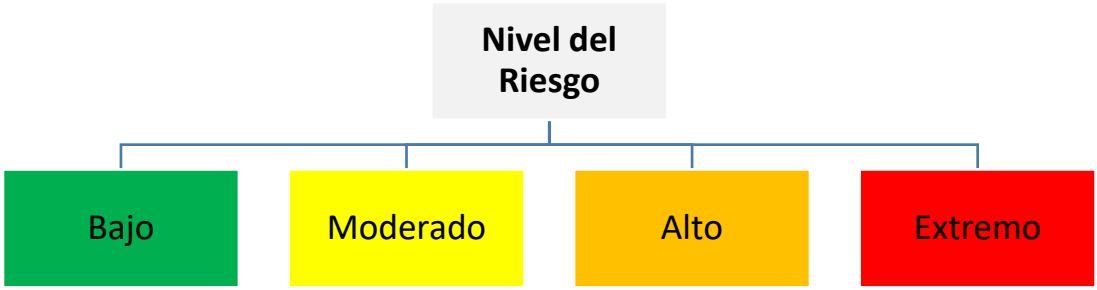
Evitar el riesgo: Se abandonan las actividades que dan lugar al riesgo, es decir, no iniciar o no continuar con la actividad que lo provoca.

Compartir el riesgo: Se reduce la probabilidad o el impacto del riesgo transfiriendo o compartiendo una parte de este. Los riesgos de corrupción se pueden compartir, pero no se puede transferir su responsabilidad. Los dos principales métodos de compartir o transferir parte del riesgo son: seguros y tercerización.

La gestión de riesgos de Seguridad y privacidad de la Información le permite a la Universidad de Cundinamarca realizar una identificación, análisis y tratamiento de los riesgos que puedan generar afectación al cumplimiento de los objetivos de los procesos, contribuyendo en la toma de decisiones, y en la prevención de la materialización de estos. La administración de riesgos de Seguridad y Privacidad de la Información se encuentra enfocada en identificar, analizar, valorar y tratar las amenazas y vulnerabilidades de los activos de información de la institución, teniendo presente su criticidad y protección, logrando un nivel de riesgo que pueda aceptar o asumir la Alta Dirección.

6. METODOLOGÍA

La identificación y valoración de riesgos sobre los activos de la información de la Universidad de Cundinamarca se encuentra detallada en la Matriz de riesgos del Sistema de Gestión de Seguridad de la Información (ESG-SSI-r039). A continuación, se discrimina el nivel de riesgo residual:



Si el riesgo se ubica en una zona no aceptable (Moderado, Alto y Extremo), se debe definir e implementar los controles necesarios para llevar el riesgo a un nivel aceptable a través del plan de tratamiento de riesgos.

6.1 IDENTIFICACIÓN DEL RIESGO

Para identificar los riesgos hay que determinar y analizar los sucesos que pueden lleguen a ocurrir y sus posibles consecuencias. Se debe considerar aspectos como infraestructura, áreas de trabajo, entorno y ambiente, para lo que se requiere que cada proceso tenga identificados sus activos de la información.

6.2 ANÁLISIS DEL RIESGO

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.

6.3 VALORACIÓN DEL RIESGO

Se establecen los criterios para analizar la probabilidad e impacto del riesgo identificado y su nivel de criticidad, con enfoque en el riesgo y su análisis que permita a los líderes de proceso contar con elementos objetivos para valorarlos y tratarlos.

En mesas de trabajo con los procesos se identifican los riesgos y se realiza el análisis de la probabilidad e impacto como valoración preliminar para identificar el nivel del riesgo inherente, asociando sus vulnerabilidades y amenazas e identificando los controles para mitigarlas.

6.4 TRATAMIENTO DEL RIESGO RESIDUAL

- **Zona de riesgo Baja:** Aceptar el riesgo.
- **Zona de riesgo Moderada:** Aceptar el riesgo, reducir el riesgo.
- **Zona de riesgo Alta:** Reducir el riesgo, evitar, transferir o compartir.
- **Zona de riesgo Extrema:** Reducir el riesgo, evitar, transferir o compartir.

Los riesgos que se encuentren en zona baja se aceptan y se continúa el monitoreo, con el fin de garantizar que las condiciones bajo las cuales han sido analizados no han cambiado, si las condiciones cambian, es necesario volver a valorar y si es el caso determinar el manejo correspondiente a través de los controles que sean necesarios. Así mismo, los riesgos de corrupción no admiten la aceptación del riesgo, siempre deben conducir a un tratamiento.

Teniendo en cuenta la aplicabilidad del ciclo PHVA, para lograr un ciclo de mejora continua en la gestión y tratamiento de riesgos, se definen las fases y las actividades, así:

Fase 1: Análisis de la información

En esta fase se revisan los resultados de las mesas de trabajo con los diferentes procesos de la institución para desarrollar las siguientes actividades:

- Verificar y analizar los riesgos identificados.
- Determinar los controles aplicables a cada riesgo.
- Definir los planes de tratamiento de los riesgos que superen el nivel de riesgo aceptable

Fase 2: Desarrollo de las medidas de tratamiento de riesgos

En esta fase se realizarán las siguientes actividades:

- Determinar la medida de tratamiento.
- Definir los responsables de cada medida.
- Desarrollar las actividades de ejecución de cada medida.

Fase 3: Análisis de los riesgos y medidas aplicadas

- Validar la eficacia de los controles y medidas de mitigación y tratamiento de los riesgos.
- Analizar la aplicabilidad de las medidas de mitigación y tratamiento de los riesgos.

Fase 4: Ciclo de vida del tratamiento de riesgos

- Definir las actividades dentro del ciclo de vida del Plan de Tratamiento de Riesgos para los riesgos Moderados, Altos y Extremos.
- Establecer las fechas para el tratamiento de los riesgos residuales no aceptables.[11]

Los riesgos que se encuentran en las zonas más altas o de mayor gravedad son los que se priorizan, determinando en el plan de contingencia las actividades de control (correctivas) que ataquen las causas del riesgo, cuando éste se llegue a materializar.

Esto ayuda a la institución a mejorar su administración de riesgos, priorizando los esfuerzos y acciones sobre los riesgos potencialmente de mayor impacto.

El Plan de Tratamiento de Riesgos contempla la definición de las actividades a desarrollar en aras de mitigar los riesgos Moderados, Altos y Extremos sobre los activos identificados en la institución, estas actividades se estructuraron de la siguiente manera, siguiendo las recomendaciones de la Guía de Gestión de Riesgos de Seguridad y Privacidad de la Información, de igual manera se encuentra documentado en el ESG-SSI-P12 "*Gestión de Riesgos de Seguridad de la Información*" y aplicado en el ESG-SSI-F039 "*Matriz de riesgos en seguridad y privacidad de la información*":

[11] Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información V.6 – MINTIC

RIESGO RESIDUAL	ACTIVIDADES	ACCIONES Y/O CONTROLES A IMPLEMENTAR	RESPONSABLE DE LA TAREA	FECHAS DE PROGRAMACIÓN DE LAS TAREAS	
				FECHA INICIO	FECHA FINAL
EXTREMO	Sensibilización	Socialización de lineamientos y herramienta para la Gestión de Riesgos de Seguridad y privacidad de la Información	Sistema de Gestión de Seguridad de la Información	02 de febrero del 2025	15 de febrero del 2025
ALTO	Identificación de Riesgos de Seguridad y Privacidad de la Información.	Identificación, Análisis y Evaluación de Riesgos de Seguridad y Privacidad de la Información.	Sistema de Gestión de Seguridad de la Información - Proceso y/o área	15 de febrero del 2025	30 de marzo del 2025
		Realimentación, revisión y verificación de los riesgos identificados (Ajustes).	Sistema de Gestión de Seguridad de la Información - Proceso y/o área	1 de abril del 2025	8 de abril del 2025
ALTO	Aceptación de riesgos identificados	Aceptación, aprobación riesgos identificados y planes de tratamiento.	Sistema de Gestión de Seguridad de la Información - Proceso y/o área	8 de abril del 2025	15 de abril del 2025
MODERADO	Publicación	Publicación de matrices de riesgos de los procesos.	Sistema de Gestión de Seguridad de la Información	15 de abril del 2025	02 de abril del 2025
ALTO	Seguimiento Fase de Tratamiento	Seguimiento implementación de controles y planes de tratamiento de riesgos los identificados	Sistema de Gestión de Seguridad de la Información	02 de abril del 2025	02 de mayo del 2025

		(verificación de evidencias).			
MODERADO	Mejoramiento	Identificación de oportunidades de mejora acorde al seguimiento de la ejecución de los controles y de los planes de tratamiento.	Sistema de Gestión de Seguridad de la Información	02 de mayo del 2025	15 de mayo del 2025
		Revisión y/o actualización de lineamientos de Riesgos de Seguridad y privacidad de la información de acuerdo con las observaciones identificadas.	Sistema de Gestión de Seguridad de la Información	15 de mayo del 2025	01 de junio del 2025
ALTO	Monitoreo y Revisión	Medición, presentación y reporte de indicadores	Sistema de Gestión de Seguridad de la Información	01 de junio del 2025	15 de junio del 2025

6.5 MONITOREO Y REVISIÓN

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.

6.6 APROBACIÓN DE LOS RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Finalizada las etapas de la identificación, actualización y gestión de Riesgos Seguridad y Privacidad de la Información y una vez diligenciado los campos requeridos y el plan de tratamiento cuando a ello haya lugar, los líderes de los procesos deberán emitir o responder con su respectiva aprobación, un correo electrónico que incluye adjunto el acta de aprobación de los riesgos y su respectiva matriz de riesgos.

7. MATERIALIZACIÓN DEL RIESGO

Cuando se detecte la materialización de riesgos por Seguridad y Privacidad de la Información, se realizarán las siguientes acciones:

1. *Materialización de riesgos detectada por parte del líder del proceso (primera línea de defensa):*

- Si el riesgo es de corrupción se deberá informar a la Oficina Asesora de Planeación como representante del Sistema de Gestión de Anticorrupción, sobre el hecho encontrado. De considerarlo necesario, realizar la denuncia ante el ente de control respectivo.

- Si el riesgo es de gestión, se debe informar al líder del proceso, para revisar la matriz de riesgos y sus controles asociados, con el fin de realizar el análisis de causas y determinar las acciones pertinentes. En caso de que se incumpla una cláusula del acuerdo de confidencialidad, se deberá escalar es caso a la Dirección de Control Disciplinario.

2. *Materialización de riesgos detectada por parte de la Dirección de Planeación segunda línea de defensa)*

- Si el riesgo es de corrupción, se deberá convocar al Comité de Control Interno e informar sobre los hechos detectados, desde donde se tomarán las decisiones para iniciar la investigación de los hechos. Dependiendo del alcance (normatividad asociada al hecho de corrupción materializado), realizar la denuncia ante el ente de control respectivo. Facilitar el inicio de las acciones correspondientes con el líder del proceso, para revisar la matriz de riesgos y sus controles asociados. Verificar si se tomaron las acciones y si se actualizó el plan de tratamiento de riesgos.

- Si el riesgo es de gestión, informar al líder del proceso sobre el hecho encontrado y orientarlo frente a la revisión, análisis y acciones correspondientes para resolver el hecho. Convocar al Comité de Coordinación de Control Interno e informar sobre la actualización realizada

8. OPORTUNIDADES DE MEJORA

Se deben identificar brechas y oportunidades de mejora en la gestión de los riesgos, considerando las apreciaciones de la Oficina de Control Interno y/o las auditorías internas y externas para optimizar la gestión de riesgos.

9. RECURSOS

La Universidad de Cundinamarca dispondrá de los siguientes recursos para gestionar los riesgos de seguridad de la información:

RECURSOS	DESCRIPCION
Humanos	• El Sistema de Gestión de Seguridad de la Información - SGSI es responsable de liderar, definir e implementar los lineamientos de seguridad de la información, estableciendo estrategias y procedimientos que contribuyan a la mejora continua de los riesgos de seguridad y privacidad de la información. • Los responsables de los procesos y áreas deben designar el personal idóneo y necesario para la identificación y gestión de riesgos de seguridad y privacidad de la información.
Técnicos	• Lineamiento de administración y gestión de riesgos del SGSI. • Herramienta para la gestión de riesgos del SGSI.
Logísticos	• Recursos y logística para la transferencia de conocimiento, socializaciones y seguimiento a la gestión de riesgos.
Financieros	• Recursos asignados al Sistema de Gestión Seguridad de la Información en la vigencia presupuestal del 2025.

10. MEDICIÓN

El monitoreo y seguimiento de los riesgos de Seguridad y Privacidad de la Información de la Universidad de Cundinamarca aprobados por los procesos, así como de sus controles y planes de tratamiento, se realiza por parte del Sistema de Gestión de Seguridad de la Información – SGSI, teniendo en cuenta la periodicidad y fechas de cumplimiento establecidas, validando los resultados de los seguimientos realizados, así como la verificación correspondiente a las evidencias de los controles definidos.

Una vez los procesos realicen el reporte de cumplimiento de sus planes de tratamiento y controles, el SGSI realizará la revisión y validación de esta información, con el fin de reportar la medición de la gestión del riesgo a través del indicador que tiene como propósito medir el nivel de implementación de los controles de los riesgos de Seguridad y Privacidad de la Información.

La medición se realiza con un indicador que está orientado principalmente a determinar el porcentaje de ejecución de los controles definidos para mitigar los riesgos identificados en los sistemas de gestión de la institución.[12]

[12] Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información V.6 – MINTIC

11. DOCUMENTOS DE REFERENCIA

- **Resolución 092 de 2023**.

  ESG-SSI-M001– Manual de lineamientos de Seguridad y Privacidad de la Información.
  ESG-SSI-G002 – Guía de Contacto con las Autoridades y Grupos de Interés Especial.

- **Procedimiento – Gestión de riesgos de seguridad de la información**

  ESG-SSI-M009 – Manual de administración de riesgos de seguridad y privacidad de la información
  ESG-SSI-F039 – Matriz de riesgos en seguridad y privacidad de la información

- **Procedimiento ESG-SSI-P01 – Gestión de activos de la información**

  ESG-SSI-M011 – Manual lineamiento de uso aceptable de activos de la información
  ESG-SSI-F034 – Consolidado del inventario de activos de la información

12. BIBLIOGRAFÍA Y WEBGRAFÍA

- 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 (2022).

- Guía para el tratamiento de riesgos de seguridad y privacidad de la información. Departamento nnnAdministrativo de la Función Pública (2024).

CONTROL DE CAMBIOS				
VERSIÓN	FECHA DE APROBACIÓN			DESCRIPCIÓN DEL CAMBIO
	AAAA	MM	DD	
1	2025	02	24	Emisión del Documento.

ELABORÓ	
NOMBRES Y APELLIDOS	CARGO
Brayan Esteban Ortegón Palomino	Técnico III

REVISÓ	
NOMBRES Y APELLIDOS	CARGO
Fabian Libardo Parra Gutiérrez	Profesional I

APROBÓ (GESTOR RESPONSABLE DEL PROCESO)				
NOMBRES Y APELLIDOS	CARGO	FECHA		
		AAAA	MM	DD
María del Pilar Delgado Rodríguez	Coordinadora del Sistema de Gestión de Seguridad de la Información	2025	02	24