1. OBJETIVO

Esta guía describe las directrices para la gestión de los riesgos para la seguridad y privacidad de la información en la Universidad Surcolombiana en función del alcance definido en el sistema de gestión de seguridad y privacidad de la información y el contexto organizacional. La gestión de riesgos y oportunidades en la Universidad Surcolombiana busca mitigar los riesgos y potencializar las oportunidades mediante el establecimiento y aplicación de lineamientos para el proceso de la gestión de los riesgos y oportunidades, a fin de contribuir al logro de los objetivos, la mejora continua del sistema de gestión y la sostenibilidad de la organización.

La gestión de riesgos de la seguridad y privacidad de la información dentro del Sistema de Gestión definido por la Universidad Surcolombiana busca garantizar la disponibilidad, confidencialidad e integridad de la información, enmarcados en el principio de crear y proteger valor.

2. ALCANCE

Los lineamientos y la metodología descrita son aplicables a todos los procesos y servicios del Sistema de Gestión de la Universidad Surcolombiana.

3. DEFINICIONES

a. Activo: todo aquello que tiene valor para la Universidad Surcolombiana.

b. Amenaza: tiene el potencial de causar daños a activos.

c. Beneficio: resultado de la gestión de oportunidades reflejado en mejoras, ventajas, rendimientos, aumento del desempeño, utilidades, eficiencia, eficacia, satisfacción, entre otros.

d. Causa: situación, falla o insuficiencia que contribuye a la materialización de un riesgo, ya sea de forma aislada o conjunta.

e. Confidencialidad: propiedad que determina que la información solo esté disponible y sea revelada a personas, entidades o procesos autorizados.

f. Consecuencia: Impacto generado por un evento o situación (favorable o adverso) que afecta los objetivos.

g. Control: medida tomada para mitigar o gestionar el riesgo, y para que la probabilidad de que la institución logre sus metas y objetivos sea mayor.

h. Disponibilidad: propiedad de que la información sea accesible y utilizable a solicitud de una persona, entidades o proceso autorizado, cuando ésta así lo requiera.

i. Evento: presencia o cambio de un conjunto particular de circunstancias. Un evento puede tener una o más ocurrencias, puede tener varias causas y puede consistir inclusive en algo que no está sucediendo. Un evento puede ser algo previsto que no llega a ocurrir, o algo no previsto que ocurre.

j. Factor de riesgo: fuente que sola o en combinación tiene potencial originador de riesgos.

k. Impacto: evaluación del efecto y la consecuencia producida al materializarse un riesgo.

l. Integridad: Propiedad de salvaguardar la exactitud y estado completo de los activos.

m. Oportunidad: circunstancia en la cual existe la posibilidad de lograr algún tipo de mejora o de obtener algún beneficio.

n. Perfil de riesgo: descripción de cualquier conjunto de riesgos y su estado. El conjunto de riesgos puede contener aquellos que se relacionan con la Institución en su totalidad, con parte de la Institución, con los procesos o servicios o según necesidad.

o. Probabilidad: variable que mide la posibilidad de que un riesgo se materialice.

p. Proceso de gestión de riesgos para la seguridad y privacidad de la información: aplicación sistemática de las políticas, los procedimientos y las prácticas de gestión a las actividades de establecimiento del contexto, evaluación de los riesgos (identificación, análisis, valoración), tratamiento, aceptación,

comunicación y consulta, vigilancia y examen de los riesgos para la seguridad y privacidad de la información

q. Riesgo: hace referencia al evento qué podría ocurrir, positivo o negativo, “que tenga un impacto directo sobre el logro de los objetivos”. También se define como un hecho, una acción u omisión que podría afectar la capacidad de la Institución para lograr sus objetivos misionales y/o estrategias. Considera la ocurrencia latente o potencial de acontecimientos negativos o inesperados, así como la ausencia o sub-aprovechamiento de oportunidades. Los riesgos positivos se tratarán como oportunidades para el Sistema de Gestión.

r. Riesgo inherente: nivel de riesgo propio de la actividad, sin tener en cuenta el efecto de los controles.

s. Riesgo residual: nivel resultante del riesgo después de aplicar los controles. Es el riesgo que queda, una vez se han aplicado los controles establecidos para su tratamiento, por lo cual requiere un permanente monitoreo de su evolución.

t. Riesgos de nivel Directivo: hace referencia a los riesgos que tienen un impacto directo sobre el cumplimiento de la planeación estratégica, con sus objetivos y planes estratégicos, así como los asuntos relativos al desempeño general de la Universidad Surcolombiana y que son relevantes para el Consejo Superior Universitario.

u. Riesgos de nivel operativo: Hace referencia a los riesgos que tengan un impacto directo sobre el cumplimiento de los objetivos de los procesos y servicios.

v. Sistema de gestión de seguridad y privacidad de la información-SGSPI: políticas, procedimientos, directrices, recursos y actividades, asociados, administrados colectivamente por la Universidad Surcolombiana, en la búsqueda de proteger sus activos de información. El SGSI es un enfoque sistemático para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad y privacidad de la información para lograr sus objetivos.

w. Vulnerabilidad: debilidad de un activo o control que puede ser explotado por una o más amenazas.

4. GENERALIDADES

4.1 MARCO DE REFERENCIA

La gestión de riesgos y oportunidades en la Universidad Surcolombiana considera para su labor, los lineamientos definidos en las políticas institucionales, además de las consideraciones definidas en:

a. La norma ISO 31000 – Gestión del riesgo. Principios y directrices.
b. La norma ISO IEC 27005 – Gestión de riesgos para la seguridad de la información.
c. Los lineamientos definidos en los documentos del Sistema de Gestión de Seguridad y Privacidad de la Información.
d. Los requisitos aplicables a la gestión del riesgo, detallados en el estándar ISO IEC 27001 y 27701
e. Código de Práctica para Controles de Seguridad de la Información - GTC ISO IEC 27002 Tecnología de la Información. Técnicas de Seguridad.
f. Modelo de Seguridad y Privacidad de la Información, Ministerio de Tecnologías y Sistemas de Información.
g. Guía de Administración de riesgos y el diseño de controles en entidades públicas

5. PROCESO DE LA GESTIÓN DEL RIESGO

El proceso de la gestión de riesgo de la seguridad y privacidad de la información está enmarcado en las siguientes etapas:

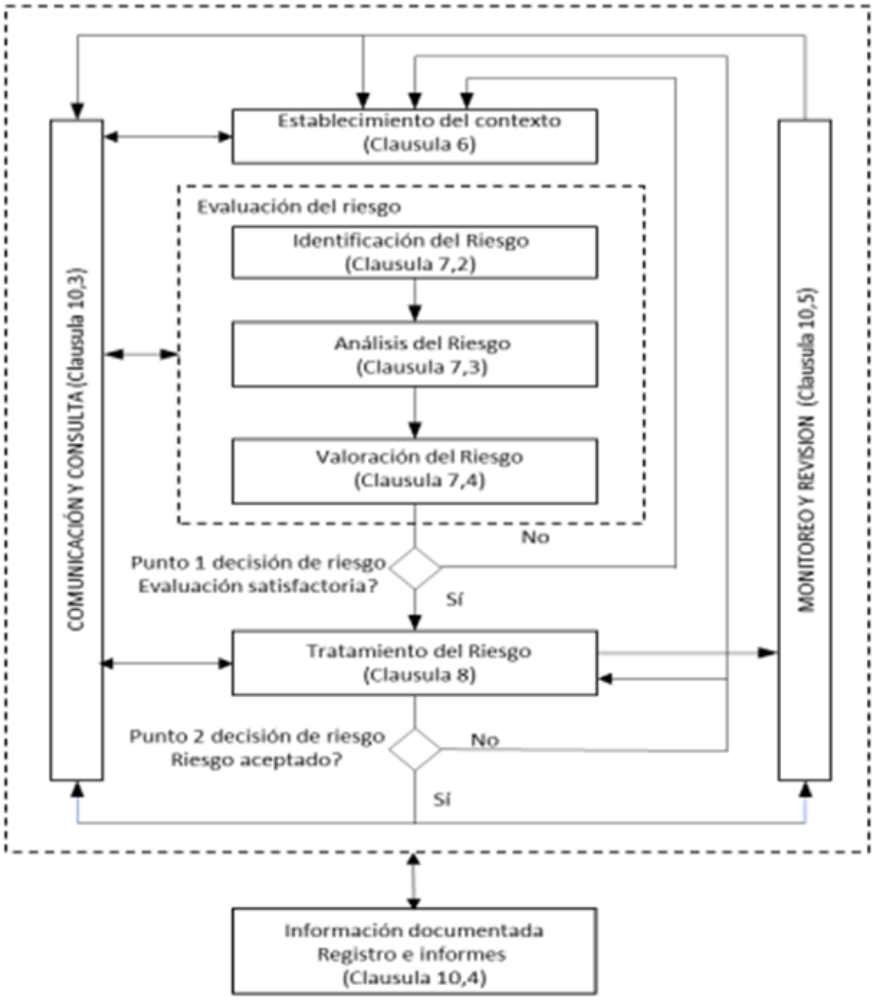
Planear
- Establecimiento del contexto
- Evaluación del riesgo
- Planificación del tratamiento del riesgo
- Aceptación del riesgo

Hacer - Implementación del plan de tratamiento de riesgo.

Verificar - Monitoreo y revisión continuos de los riesgos

Actuar - Mantener y mejorar el proceso de gestión de riesgo en la seguridad y privacidad de la información

El esquema considerado para el abordaje de la metodología de riesgos y oportunidades de la Universidad Surcolombiana se ilustra a continuación en la gráfica 1:



Gráfica 1: Proceso de gestión de riesgo en la seguridad de la información. Tomado de la norma NTC ISO IEC 27005

5.1 ESTABLECIMIENTO DEL CONTEXTO

En esta primera etapa la Universidad Surcolombiana realiza la especificación de la organización, los criterios básicos (de valoración, de impacto, de aceptación) y el alcance y los límites del proceso de gestión de los riesgos para la seguridad y privacidad de la información.

5.1.1 Roles en la gestión de riesgo

5.1.1.1 Rector

a. Identifica y comunica riesgos y oportunidades, del nivel directivo, y solicita los planes para su gestión.

b. Monitorea el comportamiento de los riesgos directivos y operativos y el perfil de riesgo institucional y pronuncia sus preocupaciones y percepciones relacionadas.

c. Aprueba la Guía para la Gestión de Riesgos y Oportunidades para la Seguridad y Privacidad de la Información, los criterios definidos para la valoración de los riesgos y participa en su revisión periódica.

d. Participa en la definición de proyectos y planes para la gestión de riesgos y oportunidades estratégicas.

e. Motiva la definición de estrategias que permitan la adopción de la cultura de riesgo en la Universidad Surcolombiana.

f. Aprueba la asignación de recursos en caso de ser necesario para la gestión del riesgo.

g. Vigila y examina los riesgos.

5.1.1.2 Comité de Seguridad y Privacidad de la Información

a. Informar a la autoridad de protección de datos cuando se presenten violaciones a los códigos de seguridad y privacidad de la información y existan riesgos en la administración de la información de los Titulares.

b. Revisar, ajustar y aprobar el Plan de Reducción de Riesgos Informáticos presentado por la Dirección del Centro de Tecnologías de Información y Comunicaciones.

c. Aprobar los niveles de aceptación del riesgo para la gestión de los riesgos de seguridad y privacidad de la información de la Universidad y revisarlos de manera periódica

5.1.1.3 Proceso de Gestión de Seguridad y Privacidad de la Información

a. Define los lineamientos e instrumentos que permiten la gestión de riesgos y oportunidades de la Universidad Surcolombiana.

b. Acompaña a los procesos en la identificación y gestión de riesgos y oportunidades y en la actualización y registro de las matrices definidas.

c. Realiza seguimiento a la gestión de riesgos y oportunidades y a las actividades derivadas, e informa cualquier desviación a los líderes de procesos.

d. Reporta los resultados de la gestión de riesgo incluidos la eficacia de los controles a la alta dirección y demás partes interesadas.
e. Desarrolla programas de capacitación relacionados con la gestión de riesgo y oportunidades.
f. Motiva la cultura de riesgo al interior de los procesos y servicios.

5.1.1.4 Líder de proceso

a. Aplica la metodología para la gestión de riesgos y oportunidades al interior de su proceso.

b. Identifica y comunica riesgos y oportunidades, de carácter operacional, y solicita los planes para su gestión.

c. Realiza control de las matrices organizacionales para su actualización y consulta.

d. Realiza seguimiento a la gestión de riesgos y oportunidades y a las actividades derivadas.

e. Reporta los resultados y la información relacionada con la gestión de riesgos y oportunidades a las partes interesadas y a la dirección en los ejercicios de revisión.

f. Motiva la cultura de riesgo al interior de su proceso o servicio.

5.1.1.5 Funcionarios administrativos, docentes, estudiantes y contratistas

a. Aplican las directrices.

b. Participan en las etapas del proceso de gestión del riesgo.

c. Promueven el desarrollo y la cultura al interior de la Universidad Surcolombiana y sus partes interesadas.

d. Reportan información relacionada con la gestión de riesgos y oportunidades al líder de su proceso.

5.1.2 Criterios Básicos

Teniendo en cuenta el alcance y los objetivos del sistema de gestión de seguridad y privacidad de la información definidos en la Universidad Surcolombiana, se han abordado los siguientes criterios básicos: criterios de evaluación del riesgo, criterios de impacto y criterios de aceptación del riesgo.

5.1.2.1 Criterios de evaluación del riesgo

Se deben considerar los siguientes aspectos con el fin de determinar los riesgos en la seguridad y privacidad de la información en la Universidad Surcolombiana:

- El valor estratégico del proceso de información de la Universidad Surcolombiana.

- La criticidad de los activos de información involucrados.
- Los requisitos legales y reglamentarios, así como las obligaciones contractuales.
- La importancia de la disponibilidad, confidencialidad e integridad para las operaciones de la Universidad Surcolombiana.
- Las expectativas y percepciones de las partes interesadas y las consecuencias negativas para el buen nombre y la reputación de la Universidad Surcolombiana.

Estos criterios son la base para determinar las prioridades para el tratamiento del riesgo.

5.1.2.2 Criterios de impacto

Los criterios de impacto deben considerar la gravedad en términos del grado de daño o de los costos para la universidad, causados por un evento de seguridad y privacidad de la información considerando los siguientes aspectos:

- Nivel de clasificación de los activos de información impactados de acuerdo a la matriz ES-GSPI-MR-05 MATRIZ DE INVENTARIO DE ACTIVOS DE LA INFORMACIÓN
- Brechas de seguridad y privacidad en la seguridad de la información (pérdida de confidencialidad, integridad y disponibilidad).
- Operaciones deterioradas (partes internas o terceras partes).
- Pérdida del negocio y el valor financiero.
- Alteración de planes y fechas límites.
- Daños para la reputación.
- Incumplimiento de los requisitos legales, reglamentarios o contractuales.

5.1.2.3 Criterios de aceptación del riesgo

La Universidad Surcolombiana ha definido los siguientes aspectos para los niveles de aceptación de riesgo:

- La alta dirección de la Universidad Surcolombiana ha definido como umbral aceptable de riesgo todos aquellos que se encuentren por debajo de la zona de riesgo externo. Podrían aceptarse riesgos por encima de este nivel en circunstancias específicas.

- Siempre se debe considerar la relación entre el beneficio estimado y el riesgo estimado.
- Cualquier riesgo relacionado con el incumplimiento de aspectos legales y reglamentarios no es aceptado en la Universidad Surcolombiana.
- Dependiendo de la naturaleza del riesgo se podrían incluir actividades de tratamiento futuras siempre y cuando haya un compromiso para ejecutar acciones que reduzcan dicho riesgo hasta un nivel aceptable en un periodo definido de tiempo.

Los criterios de aceptación en la Universidad Surcolombiana consideran los siguientes elementos:

- Criterios de la Universidad Surcolombiana
- Aspectos legales y reglamentarios
- Operaciones
- Tecnología
- Finanzas
- Factores sociales y humanitarios.

5.1.3 Alcance y límites de la gestión de riesgos de la seguridad y privacidad de la información

5.1.3.1 Análisis del contexto para la organización

El establecimiento del contexto en la Universidad Surcolombiana involucra el conocimiento de la organización y de su entorno interno y externo, que es tenido en cuenta en la identificación de los riesgos y oportunidades aplicables; además permite la definición del alcance de la gestión de riesgo, el establecimiento de los factores de riesgo considerados en la identificación, las tipologías de riesgo y los criterios de calificación definidos y su valoración.

Para establecer y analizar el contexto organizacional, la Universidad Surcolombiana dispone de los formatos ES-GSPI-MR-01 MATRIZ DE CONTEXTO DE LA ORGANIZACIÓN y ES-GSPI-MR-03 MATRIZ IDENTIFICACIÓN DE PARTES INTERESADAS PERTINENTES SGSPI, en el cual se detallan los elementos, herramientas y responsables dispuestos para este propósito, además de la información y de los factores claves a considerar.

5.1.3.2 Delimitación del alcance de la gestión de riesgo

La gestión de riesgo en la Universidad Surcolombiana considera los niveles directivos y operativos que incluyen los riesgos de los procesos que conforman el sistema de gestión, y los riesgos de los proyectos de innovación, en toda su operación.

Cada vez que se desarrollen proyectos de innovación e investigación es necesario identificar y valorar los riesgos asociados con el líder de proyecto asignado. Las actividades consideradas para este propósito están definidas en el procedimiento

El alcance definido para la gestión de riesgo de la seguridad y privacidad de la información está relacionado con el alcance definido para seguridad y privacidad de la información en el documento MANUAL DE GESTIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

5.1.3.3 Gestión de las oportunidades

La gestión de las oportunidades permite a la Universidad Surcolombiana la adopción de nuevas prácticas para la mejora del desempeño, el diseño y desarrollo de nuevos servicios, la apertura de nuevos mercados, el acercamiento a nuevos clientes, el establecimiento de nuevas alianzas o convenios, la implementación de nuevas tecnologías y todos aquellos posibles escenarios que le permitan abordar sus necesidades y los objetivos misionales institucionales.

Las oportunidades identificadas a partir del análisis de contexto de la organización, del análisis y monitoreo del mercado o del análisis interno de los procesos, entre otros; son gestionadas en la Universidad Surcolombiana considerando lo siguiente:

a. Cuando se presenten oportunidades asociadas con los objetivos estratégicos de la Universidad Surcolombiana

b. Cuando se presenten oportunidades asociadas con el establecimiento de alianzas, asociaciones o acuerdos de cooperación

c. Cuando se presenten oportunidades asociadas a la adopción de nuevas prácticas o lanzamiento de nuevas ofertas académicas y servicios educativos

d. Cuando se presenten oportunidades asociadas a la apertura de nuevos mercados, acercamiento a nuevos clientes y demás temas comerciales

e. Cuando se presenten oportunidades asociadas con la utilización de herramientas tecnológicas

f. Cuando se presenten oportunidades asociadas a la Mejora del Sistema de Gestión

6. EVALUACIÓN DEL RIESGO

En esta segunda etapa la Universidad Surcolombiana realiza una lista de riesgos evaluados y priorizados según los criterios de valoración de riesgos

6.1 IDENTIFICACIÓN DEL RIESGO

Para la identificación del riesgo se seleccionan de la matriz se deben considerar los siguientes elementos definidos en el capítulo 3 de este documento referenciado a los activos que tiene criticidad ALTA, y registrarlos en el formato ES-GSPI-MR-06 MATRIZ DE RIESGO SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

Activo
Amenaza
Control
Vulnerabilidad
Consecuencia

La Universidad Surcolombiana utiliza como guía de referencia la norma NTC ISO IEC 27005:2020 en sus anexos para el proceso de identificación de riesgos.

Los activos de información se clasifican en dos tipos:

a) Primarios:

a. Actividades y procesos del negocio: procesos cuya pérdida o degradación hacen imposible llevar a cabo la misión institucional; procesos que contienen procesos secretos o que implican tecnología propietaria; procesos que, si se modifican,

pueden afectar de manera muy significativa el cumplimiento de la misión de la Universidad; procesos que son necesarios para el cumplimiento de los requisitos contractuales, legales o reglamentarios.

b. Información: información vital para la ejecución de la misión institucional; información personal que se puede definir específicamente en el sentido de las leyes relacionadas con la privacidad; información estratégica que se requiere para alcanzar los objetivos determinados por las orientaciones estratégicas; información del alto costo cuya recolección, almacenamiento, procesamiento y transmisión exigen un largo periodo de tiempo y/o implican un alto costo de adquisición, etc.

b) De Soporte

a. Hardware: consta de todos los elementos físicos que dan soporte a los procesos (PC, portátiles, servidores, impresoras, discos, documentos en papel, etc.).

b. Software: consiste en todos los programas que contribuyen al funcionamiento de un conjunto de procesamiento de datos (sistemas operativos, paquetes de software o estándar, aplicaciones, mantenimiento o administración, etc.)

c. Redes: Consiste en todos los dispositivos de telecomunicaciones utilizados para interconectar varios computadores remotos físicamente o los elementos de un sistema de información (conmutadores, cableado, puntos de acceso, etc.)

d. Personal: consiste en todos los grupos de personas involucradas en el sistema de información (usuarios, desarrolladores, responsables, etc.)

e. Ubicación: comprende todos los lugares en los cuales se pueden aplicar los medios de seguridad de la organización (Edificios, salas, y sus servicios, etc.)

f. Estructura organizativa: responsables, dependencias, contratistas, etc.

6.2 ANÁLISIS DEL RIESGO

Los criterios de calificación para cada uno de los riesgos en términos de posibilidad e impacto se definen en las siguientes tablas:

Estimación del Riesgo: POSIBILIDAD			
Posibilidad	**Valor**	**Descripción**	**Frecuencia**
Casi Seguro	A	Se espera que ocurra en la mayoría de las circunstancias	Más de 1 vez al año.
Probable	B	El evento probablemente ocurrirá en la mayoría de las circunstancias,	Al menos de 1 vez en El último año.
Posible	C	El evento podría ocurrir en algún momento.	Al menos de 1 vez en Los últimos 2 años.
Improbable	D	Es muy poco factible que el evento se presente.	Al menos de 1 vez en Los últimos 5 años.
Raro	E	El evento puede ocurrir sólo en circunstancias excepcionales.	No se ha presentado en los últimos 5 años

Tabla 1 Estimación del riesgo: POSIBILIDAD

Estimación del Riesgo: CONSECUENCIA - IMPACTO		
Impacto	**Valor**	**Descripción**
Insignificante	1	La materialización del riesgo **puede ser controlado** por los participantes del proceso, y **no afecta los objetivos del proceso**.
Menor	2	La materialización del riesgo ocasiona **pequeñas demoras** en el cumplimiento de las actividades del proceso, y **no afecta significativamente el cumplimiento de los objetivos** de la Universidad. Tiene un impacto bajo en los procesos de otras áreas de la Universidad Surcolombiana.
Moderado	3	La materialización del riesgo **demora el cumplimiento de los objetivos del proceso,** y tiene un **impacto moderado en los procesos de otras áreas** de la Universidad. Puede además causar un deterioro en el desarrollo del proceso dificultando o retrasando el cumplimiento de sus objetivos, impidiendo que éste se desarrolle en forma normal.

Mayor	4	La materialización del riesgo **retrasa el cumplimiento de los objetivos de la Universidad** y tiene un **impacto significativo en su imagen pública**. Puede además generar impactos en: la industria; sectores económicos, el cumplimiento de acuerdos y obligaciones legales nacionales e internacionales; multas y las finanzas públicas; entre otras
Catastrófico	5	La materialización del riesgo **imposibilita el cumplimiento de los objetivos de la** Universidad, tiene un **impacto catastrófico en su imagen pública**. Puede además generar impactos en: sectores económicos, los mercados; la industria, el cumplimiento de acuerdos y obligaciones legales nacionales e internacionales; multas y las finanzas públicas; entre otras.

Tabla 2 Estimación del riesgo: CONSECUENCIA IMPACTO

6.3 EVALUACIÓN DEL RIESGO

La Universidad Surcolombiana ha definido 4 zonas: extremo, alto, medio, bajo en términos de la posibilidad de ocurrencia de sus riesgos y el impacto de sus consecuencias.

De acuerdo a los criterios definidos en el análisis, la Universidad Surcolombiana representa gráficamente la ubicación de sus riesgos en el siguiente gráfico:

EVALUACION DEL RIESGO - CONSECUENCIA NEGATIVA					
POSIBILIDAD	**IMPACTO**				
	Insignificante (1)	Menor (2)	Moderado (3)	Mayor (4)	Catastròfico (5)
Casi seguro (A)	A	A	E	E	E
Probable (B)	M	A	A	E	E
Posible (C)	B	M	A	E	E
Improbable (D)	B	B	M	A	E
Raro (E)	B	B	M	A	A

Tabla 3. Esquema general de Matriz de Riesgo Institucional y Zonas de Riesgo Institucional

Las zonas de riesgo se diferencian por colores y por número de la zona de la siguiente manera:

B: Zona de riesgo baja: Asumir el riesgo
M: Zona de riesgo moderado: Asumir el riesgo, reducir el riesgo
A: Zona de riesgo Alta: Reducir el riesgo, evitar, compartir o transferir
E: Zona de riesgo extrema: Reducir el riesgo, evitar, compartir o transferir

Tabla 4. Convención Zonas de Riesgo

El análisis del riesgo permite además identificar oportunidades de mejora, cuando la consecuencia es positiva:

EVALUACION DEL RIESGO - CONSECUENCIA POSITIVA					
POSIBILIDAD	IMPACTO				
	Insignificante (1)	Menor (2)	Moderado (3)	Mayor (4)	Catastròfico (5)
Casi seguro (A)	A	A	E	E	E
Probable (B)	M	A	A	E	E
Posible (C)	B	M	A	E	E
Improbable (D)	B	B	M	A	E
Raro (E)	B	B	M	A	A

Tabla 5. Esquema general de Matriz de oportunidad institucional y zonas de oportunidad institucional

Las zonas de oportunidad se diferencian por colores y por número de la zona de la siguiente manera:

B: Zona de oportunidad baja: Asumir la oportunidad
M: Zona de oportunidad moderada: Asumir la oportunidad.
A: Zona de oportunidad Alta: Aumentar la posibilidad de ocurrencia, compartir o transferir
E: Zona de oportunidad extrema: Aumentar la posibilidad de ocurrencia y/o el impacto de la oportunidad, asumir, compartir o transferir.

Tabla. Convención Zonas de Oportunidad

Para esta etapa el Comité de Seguridad y Privacidad de la Información de la Universidad Surcolombiana realiza un análisis de los riesgos teniendo en cuenta los criterios definidos en la etapa de contexto, seleccionando de manera prioritaria para su tratamiento aquellas que representen una amenaza y/o oportunidad significativa

para sus activos de información. (Zona de riesgos extrema y Zona de oportunidad extrema).

6.4 TRATAMIENTO DEL RIESGO

En esta tercera etapa la Universidad Surcolombiana define los planes de tratamiento de riesgos y riesgos residuales.

Las opciones de tratamiento definidas en la Universidad Surcolombiana son:

- Evitar el riesgo: decisión de no involucrarse en una situación de riesgo o tomar acción para retirarse de dicha situación.
- Retención del riesgo: aceptación de la pérdida o ganancia proveniente de un riesgo particular.
- Reducción del riesgo: acciones que se toman para disminuir la probabilidad, las consecuencias negativas, o ambas, asociadas a un riesgo.
- Transferencia del riesgo: compartir con otras partes la pérdida o la ganancia de un riesgo.

Para el tratamiento del riesgo es importante tener en cuenta la relación costo beneficio:

- El nivel de riesgo está muy alejado del nivel de tolerancia, su costo y tiempo del tratamiento es muy superior a los beneficios.
- El costo del tratamiento por parte de terceros (internos o externos) es más beneficioso que el tratamiento directo
- El costo y el tiempo del tratamiento es adecuado a los beneficios
- La implementación de medidas de control adicionales no generará valor agregado para reducir niveles de ocurrencia o de impacto.

6.5 ACEPTACIÓN DEL RIESGO

Para la aceptación del riesgo la alta dirección debe utilizar los criterios de aceptación del riesgo definidos en el capítulo 5.1.2.3 de este documento.

En esta cuarta etapa se determina una lista de los riesgos aceptados con la justificación de los que no cumplen con los criterios normales de aceptación de riesgos de la Universidad.

6.6 COMUNICACIÓN DEL RIESGO

La Universidad Surcolombiana ha definido actividades a través del proceso de comunicaciones (ES-CMU-MR-01) Matriz de comunicaciones de la Universidad para intercambiar y compartir información acerca del riesgo entre la organización y las diferentes partes interesadas facilitando la comprensión continua del proceso y los resultados de la gestión para la seguridad y privacidad de la información de la organización

6.7 VIGILANCIA Y REVISIÓN DE LOS RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Esta actividad busca la alineación continua de la gestión de riesgos con los objetivos de la Universidad Surcolombiana, con los criterios de aceptación de riesgos y la pertinencia continua del proceso de gestión de riesgos para la seguridad y privacidad de la información.

Para ello se ha definido que la frecuencia de vigilancia y revisión sea anual.

CONTROL DE CAMBIOS

VERSIÓN	DOCUMENTO Y FECHA DE APROBACIÓN	DESCRIPCION DE CAMBIÓS
01	EV-CAL-FO-17 del 24 de noviembre de 2025	Creación del documento.

ELABORÓ	REVISÓ	APROBÓ
MARTHA LILIANA HERMOSA TRUJILLO Coordinador Sistema Gestión de Seguridad y Privacidad de la Información.	LAURA LORENA PÉREZ CALDERÓN Profesional SGC	MAYRA ALEJANDRA BERMEO BALAGUERA Coordinador SGC