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

Control de Cambios

Version	Fecha	Descripción	Elaboró
1.0	30-01-2020	Version Inicial	Mag. Martha Liliana Hermosa Trujillo Ing. Isabel Cristina Cleves Rodriguez
2.0	26-01-2021	Actualización	Mag. Martha Liliana Hermosa Trujillo Ing. Isabel Cristina Cleves Rodriguez Mag. Germán Andrés Sánchez Ortegon

TABLA DE CONTENIDO

TABLA DE GRAFICAS

TABLA DE CUADROS

1. INTRODUCCIÓN

Hoy día, todas las instituciones están inmersas en la denominada revolución digital y esto hace que reconozcan la importancia de la información en sus procesos misionales y la importancia de tener su información interna bien identificada y protegida, al igual que la proporcionada por sus partes interesadas, enmarcada bajo las relaciones de cumplimiento, comerciales y contractuales como los son acuerdos de confidencialidad y demás compromisos, que obligan a dar un tratamiento, manejo y clasificación a la información bajo una correcta administración y custodia.

La Seguridad de la Información en las instituciones tiene como objetivo la protección de los activos de información en cualquiera de sus estados ante una serie de amenazas o brechas que atenten contra sus principios fundamentales de confidencialidad, integridad y su disponibilidad, a través de la implementación de medidas de control de seguridad de la información, que permitan gestionar y reducir los riesgos e impactos a que está expuesta y se logre alcanzar el máximo retorno de las inversiones en las oportunidades de negocio.

El plan de tratamiento de riesgos de Seguridad y Privacidad de la información, Seguridad y Continuidad de la Operación, se basa en una orientación estratégica que requiere el desarrollo de una cultura de carácter preventivo, de manera que, al comprender el concepto de riesgo, así como el contexto, se planean acciones que reduzcan la afectación a la entidad en caso de materialización, adicional se busca desarrollar estrategias para la identificación, análisis, tratamiento, evaluación y monitoreo de dichos riesgos con mayor objetividad, dando a conocer aquellas situaciones que pueden comprometer el cumplimiento de los objetivos institucionales.

Con lo anterior, la Universidad da cumplimiento a la normatividad nacional en estos temas como lo son el CONPES 3854 de 2016, el Modelo de Seguridad y Privacidad de la Información de la Universidad Surcolombiana, el decreto 1008 de 14 de junio 2018, adoptando las buenas prácticas y los lineamientos de los estándares NTC ISO IEC 27001, NTC ISO 31000 entre otros.

Los principios de protección de la información se enmarcan en:

- **Confidencialidad**: propiedad que la información sea concedida únicamente a quien esté autorizado.
- **Integridad**: propiedad que la información se mantenga exacta y completa.
- **Disponibilidad**: propiedad que la información sea accesible y utilizable en el momento que se requiera.

2. OBJETIVO

Brindar a la Universidad Surcolombiana una herramienta con enfoque sistemático que le permita definir y aplicar los lineamientos para tratar de manera integral los riesgos de Seguridad y Privacidad de la Información, a que pueda estar expuesta, y de esta manera alcanzar los objetivos, la misión y la visión institucional, protegiendo y preservando la integridad, confidencialidad y disponibilidad de la información.

2.1. OBJETIVOS ESPECIFICOS DE LA GUÍA METODOLÓGICA DE RIESGOS

- ✓ Brindar lineamientos y principios que propendan por la unificación de criterios para la administración de los riesgos de seguridad de la información.

- ✓ Fortalecer el sistema de gestión de riesgos de la Universidad Surcolombiana incorporando controles y medidas de seguridad de la información que estén acordes al entorno operativo de la Institución.

- ✓ Proteger el valor de los activos de información mediante el control de implementación de acciones de mitigación frente al riesgo y potencializar las oportunidades asociadas

- ✓ Generar una cultura y apropiación de trabajo enfocada a la identificación de los riesgos de seguridad de la información, y su mitigación.

- ✓ Reducir toda posibilidad de que una brecha o evento produzca determinado impacto bien en la información o cualquier otro activo de información asociado, a través de la gestión adecuada de los riesgos de la seguridad de la información.

- ✓ Lograr y mantener a través de la implementación de medidas de control el nivel de probabilidad/posiblidad e impacto residual de los riesgos a el nivel aceptable por parte de la Dirección de la Universidad.

3. ALCANCE

La gestión de riesgos de seguridad de la información y su tratamiento, será aplicada sobre cualquier proceso de la Universidad Surcolombiana y cualquier activo de información de la Institución que se vea afectado en su disponibilidad, integridad, confidencialidad, a través de los principios básicos y metodológicos para la gestión de los riesgos de seguridad de la información, así como las técnicas, actividades y formularios que permitan y faciliten el desarrollo de las etapas de reconocimiento del contexto, identificación de los riesgos de seguridad de la información , análisis y evaluación, opciones de tratamiento o manejo del riesgo según la zona de riesgo; incluye además pautas y recomendaciones para su seguimiento, monitoreo y evaluación.

Realizar una eficiente gestión de riesgos de Seguridad y Privacidad de la información de manera que permita integrar en los procesos de la Universidad, buenas prácticas que contribuyan a la toma de decisiones y prevengan incidentes que puedan afectar el logro de los objetivos institucionales.

Para el Plan de Tratamiento de Riesgos se tendrán en cuenta los riesgos que se encuentren en niveles alto y extremo, los criterios para la evaluación y aceptación de riesgos acorde con los lineamientos definidos por la Universidad, los riesgos que se encuentren en niveles inferiores serán aceptados por la Universidad.

4. MARCO NORMATIVO Y REFERENCIA

Los siguientes documentos de referencia, normativos, vinculantes hacen parte integral del presente documento, sus consideraciones, alcance y construcción:

- **Constitución Política de Colombia 1991**. Artículo 15. Reconoce como Derecho Fundamental el Habeas Data. Artículo 20. Libertad de Información.
- **Decreto 612 de 2018,** Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las Entidades del Estado.
- **Decreto 1008 de 2018**, Por el cual se establecen los lineamientos generales de la política de Gobierno Digital.
- **Ley 23 de 1982** de Propiedad Intelectual - Derechos de Autor.
- **Ley 594 de 2000** - Ley General de Archivos.
- **Ley 527 de 1999**, por la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales y se

establecen las entidades de certificación y se dictan otras disposiciones.

- **Ley Estatutaria 1266 de 2008**, por la cual se dictan disposiciones generales del Habeas Data y se regula el manejo de la información contenida en base de datos personales.
- **Ley 1273 de 2009**, "Delitos Informáticos" protección de la información y los datos.
- **Ley 1437 de 2011**, "Código de procedimiento administrativo y de lo contencioso administrativo".
- **Ley 1581 de 2012**, "Protección de Datos personales".
- **Decreto 2609 de 2012**, por la cual se reglamenta la ley 594 de 200 y ley 1437 de 2011
- **Decreto 1377 de 2013**, por la cual se reglamenta la ley 1581 de 2012
- **Ley 1712 de 2014,** "De transparencia y del derecho de acceso a la información pública nacional"
- **Ley 962 de 2005**. "Simplificación y Racionalización de Trámite. Atributos de seguridad en la Información electrónica de entidades públicas;"
- **Ley 1150 de 2007**. "Seguridad de la información electrónica en contratación en línea"
- **Ley 1341 de 2009**. "Tecnologías de la Información y aplicación de seguridad".
- **Decreto 2952 de 2010**. "Por el cual se reglamentan los artículos 12 y 13 de la Ley 1266 de 2008"
- **Decreto 886 de 2014**. "Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012"
- **Decreto 1083 de 2015**. "Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012"
- **CONPES 3701 de 2011** Lineamientos de Política para Ciberseguridad y Ciberdefensa
- **CONPES 3854 de 2016** Política Nacional de Seguridad digital.
- **Resolución 79B de 2020.** Por la cual se crea el Comité de Seguridad de la Información de la Universidad Surcolombiana
- **Resolución 289 de 2019.** Por la cual se adopta la Política General del Modelo de Seguridad y Privacidad de la Información y el Manual de la Política Seguridad y Privacidad de la Información de la Universidad Surcolombiana
- **Resolución 290 de 2019.** Por la cual se adopta la Política de tratamiento y Protección de datos personales de la Universidad Surcolombiana
- **Resolución P4042 de 2019.** Por medio de la cual se crea, organiza y conforma un grupo interno de trabajo de seguridad de la Información y Protección de Datos personales y se asignan funciones de coordinador a un empleado público de la Universidad Surcolombiana

4. REQUISITOS TÉCNICOS

- NTC ISO IEC 27001 Sistemas de gestión de la seguridad de la información
- GTC ISO IEC 27002 Tecnología de la Información. Técnicas de Seguridad. Código de Práctica para Controles de Seguridad de la Información
- NTC ISO lEC 27005 Tecnología de la Información. Técnicas de Seguridad. Gestión del Riesgo en la Seguridad de la Información.
- NTC ISO 19011 Directrices para la Auditoria de los Sistemas de Gestión.
- Modelo de Seguridad y Privacidad de la Información, Ministerio de Tecnologías y Sistemas de Información.
- Guía para la administración del riesgo y el diseño de controles en entidades públicas - Versión 5 - Diciembre de 2020

5. POLÍTICA DE ADMINISTRACION DE RIESGOS

El Comité de Seguridad de la Información de la Universidad Surcolombiana, a través del sistema de gestión de seguridad de la información, se compromete a mantener la cultura de la gestión de riesgos asociados, con la responsabilidad de diseñar, adoptar y promover las políticas, planes, programas y proyectos de TI, gestionando los riesgos de los procesos y proyectos, mediante mecanismos, sistemas y controles enfocados a la prevención y detección de amenazas asociadas a los activos de información que comprometan la disponibilidad, confidencialidad e integridad, fortaleciendo las medidas de control de manera continua y oportuna

La política define los lineamientos para la gestión de los riesgos y establece pautas de acción necesarias para todos los funcionarios administrativos, docentes, contratistas y/o terceros que requieran acceso a los sistemas de información o aplicaciones de la Universidad Surcolombiana.

Las opciones para el tratamiento del riesgo se deben seleccionar con base en el resultado de la valoración del riesgo, el costo esperado de implementar estas opciones y los beneficios esperados como resultado de tales opciones.

Las siguientes son las alternativas planteadas para el tratamiento del riesgo:

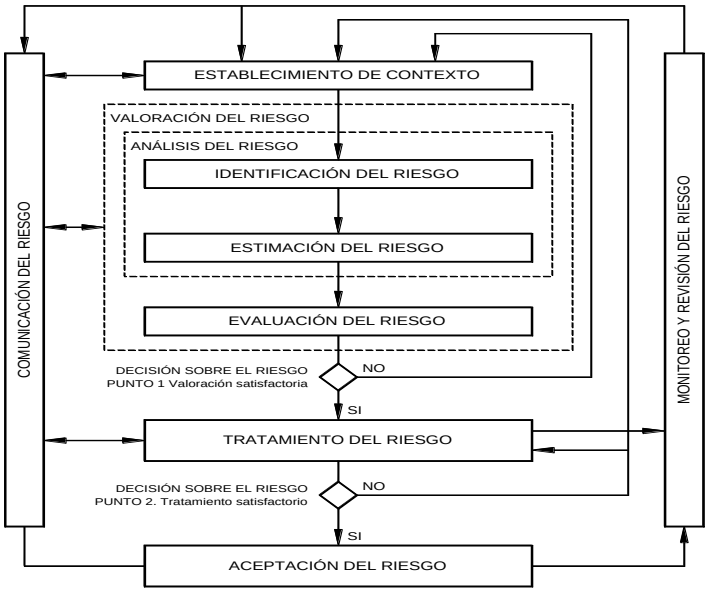
- **Reducir o Mitigar el riesgo.** Acciones que se toman para disminuir la probabilidad las consecuencias negativas, o ambas, asociadas con un riesgo, mediante la selección de controles, de manera tal que el riesgo residual se pueda reevaluar como aceptable.

- **Retener o Aceptar el riesgo.** Aceptación de la pérdida o ganancia proveniente de un riesgo particular. La decisión sobre la retención sin acción posterior se debe tomar dependiendo la evaluación del riesgo.
- **Evitar el riesgo.** Decisión de no involucrarse en una situación de riesgo o tomar acción para retirarse de dicha situación, se debe evitar la actividad o acción que da origen al riesgo en particular.
- **Transferir o Compartir el riesgo.** Compartir con otra de las partes la pérdida o la ganancia de un riesgo. El riesgo se debe transferir a otra persona que pueda gestionar de manera más eficaz el riesgo en particular dependiendo la evaluación del riesgo.

6. VISION GENERAL DEL PROCESO DE GESTION DE RIESGO EN LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

A continuación, se presenta el modelo de gestión de riesgos de seguridad de la información diseñada basada en la norma NTC ISO IEC 27005 para la adecuada administración de riesgos en la seguridad de la información; los elementos que lo componen son:

La gestión de riesgos de seguridad de la información deberá ser iterativa para las actividades de valoración de riesgos y/o tratamiento de estos.



Grafica 1. Proceso de gestión de riesgo en la seguridad y privacidad de la información. Tomado de la norma NTC ISO IEC 27005

a. ESTABLECIMIENTO DEL CONTEXTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El contexto de gestión de riesgos de seguridad de la información define los criterios básicos que serán necesarios para enfocar el ejercicio por parte de la Universidad Surcolombiana y obtener los resultados esperados, basándose en, la identificación de las fuentes que pueden dar origen a los riesgos y oportunidades en sus procesos, en el análisis de las debilidades y amenazas asociadas, en la valoración de los riesgos en términos de sus consecuencias y en la probabilidad de su ocurrencia, al igual que en la construcción de acciones de mitigación en beneficio de lograr y mantener niveles de riesgos aceptables para la Universidad.

Como criterios para la gestión de riesgos de seguridad de la información se establecen:

i. Criterios de evaluación del riesgo de seguridad de la información:

La evaluación de los riesgos de seguridad de la información se enfocará en:

- El valor estratégico del proceso de información en 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, integridad y confidencialidad para las operaciones de la Universidad Surcolombiana.
- Las expectativas y percepciones de las partes interesadas y las consecuencias negativas para el buen nombre y reputación de la Universidad Surcolombiana.

ii. Criterios de Impacto

Los criterios de impacto se especificarán en términos del grado, daño o de los costos para la Universidad Surcolombiana, causados por un evento de seguridad de la información, considerando aspectos tales como:

- Nivel de clasificación de los activos de información impactados

- Brechas en la seguridad de la información (pérdida de la confidencialidad, integridad y disponibilidad)
- Operaciones deterioradas (afectación a partes internas o terceras partes)
- Pérdida del negocio y del valor financiero
- Alteración de planes o fechas límites
- Daños en la reputación
- Incumplimiento de los requisitos legales, reglamentarios o contractuales

iii. Criterios de Aceptación

Los criterios de aceptación dependerán con frecuencia de las políticas, metas, objetivos de la Universidad Surcolombiana y de las partes interesadas.

b. VALORACIÓN DE LOS RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Los riesgos se deberán identificar, describir cuantitativamente o cualitativamente y priorizarse frente a los criterios de evaluación del riesgo y los objetivos relevantes para la Universidad Surcolombiana, esta fase consta de las siguientes etapas:

La valoración del Riesgo de seguridad de la información consta de las siguientes actividades:

- Análisis del riesgo

  - ✓ Identificación de los riesgos
  - ✓ Estimación del riesgo

- Evaluación del riesgo

i. Identificación de riesgos y oportunidades

Para la evaluación de riesgos de seguridad de la información en primer lugar se deben identificar los activos de información por proceso en evaluación.

7.2.1.1 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.

Una vez identificados los activos de información se deben priorizar de acuerdo a su impacto sobre el sistema de gestión de seguridad de la información (valor económico, confidencialidad, integridad y disponibilidad).

7.2.1.2 Identificación de amenazas, controles y vulnerabilidades

Después de haber identificado los activos de información y de tener el resultado de la priorización del impacto sobre el sistema de gestión de la seguridad de la información, se deben identificar las amenazas que pueden causar daños en los activos de información primarios y/o de soporte de mayor impacto. La identificación de las amenazas y la valoración de los daños que pueden producir se puede obtener preguntando a los propietarios de los activos, usuarios, expertos, etc.

Posterior a la identificación del listado de activos, sus amenazas y los controles y medidas que ya se han tomado, a continuación, se revisarán las vulnerabilidades que podrían aprovechar las amenazas y causar daños a los activos de información de la Universidad Surcolombiana. Existen distintos métodos para analizar amenazas, por ejemplo:

- Entrevistas con líderes de procesos y usuarios
- Inspección física
- Uso de las herramientas para el escaneo automatizado

Para cada una de las amenazas analizaremos las vulnerabilidades (debilidades) que podrían ser explotadas.

Finalmente se identificarán las consecuencias, es decir, cómo estas amenazas y vulnerabilidades podrían afectar la confidencialidad, integridad y disponibilidad de los activos de información.

ii. Estimación del riesgo

La estimación del riesgo busca establecer la probabilidad/posibilidad de ocurrencia de los riesgos y el impacto de sus consecuencias, calificándolos y evaluándolos con el fin de obtener información para establecer el nivel de riesgo, su priorización y estrategia de tratamiento de estos. El objetivo de esta etapa es el de establecer una valoración y priorización de los riesgos.

Para adelantar la estimación del riesgo se deben considerar los siguientes aspectos:

- **Posibilidad**: la posibilidad de ocurrencia del riesgo, representa el número de veces que el riesgo se ha presentado en un determinado tiempo o pudiese presentarse y que tan posible es que la amenaza explote la vulnerabilidad sobre el activo de información.

- **Impacto**: hace referencia a las consecuencias que puede ocasionar a la Universidad Surcolombiana la materialización del riesgo; se refiere a la magnitud de sus efectos.

Se sugiere realizar este análisis con todas o las personas que más conozcan del proceso, y que por sus conocimientos o experiencia puedan determinar el impacto y la posibilidad del riesgo de acuerdo con los rangos señalados en las tablas que se muestran más adelante.

Como criterios para la estimación del riesgo desde el enfoque de impacto y consecuencias se podrán tener en cuenta: pérdidas financieras, costes de reparación o sustitución, interrupción del servicio, disminución del rendimiento, infracciones legales, pérdida de ventaja competitiva, daños personales, entre otros.

Además de medir las posibles consecuencias se deberán analizar o estimar la probabilidad de ocurrencia de situaciones que generen impactos sobre los activos de información o la operación del negocio.

Para realizar el análisis de riesgo de un proceso, se deberá calificar el impacto y la posibilidad de cada uno de los riesgos identificados de acuerdo con los niveles para la estimación de los riesgos los cuales pueden ser valorados de manera cualitativa y/o cuantitativa.

Para la estimación de la posibilidad se van a utilizar la metodología de valoración cualitativa:

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. Valoración Posibilidad.

Para la estimación de la consecuencia/impacto se va a utilizar la metodología de valoración cuantitativa:

Estimación del Riesgo: CONSECUENCIA - IMPACTO		
Posibilidad	**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 Surcolombiana. 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 Surcolombiana. 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 Surcolombiana** y tiene un **impacto significativo en la imagen pública** de la Universidad Surcolombiana. 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 Surcolombiana, tiene un **impacto catastrófico en la imagen pública de la** Universidad Surcolombiana. 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. Valoración Impacto

iii. Determinación del riesgo inherente y residual

El análisis del riesgo determinado por su posibilidad e impacto permite tener una primera evaluación del riesgo inherente (escenario sin controles) y ver el grado de exposición al riesgo que tiene la Universidad Surcolombiana. La exposición al riesgo es la ponderación de la posibilidad e impacto, y se puede ver gráficamente en la matriz de riesgo, instrumento que muestra las zonas de riesgos y que facilita el análisis gráfico. Permite analizar de manera global los riesgos que deben priorizarse según la zona en que quedan ubicados los mismos (zona de riesgo bajo, moderado, alto o extremo) facilitando la organización de prioridades para la decisión del tratamiento e implementación de planes de acción.

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 6. Convención Zonas de Oportunidad

iv. Evaluación de los riesgos

Una vez se valoran los impactos, la posibilidad y las consecuencias de los escenarios de incidentes sobre los activos de información, se obtendrán los niveles de riesgo y oportunidades, para los cuales se deberán comparar frente a los criterios de evaluación definidos en el contexto, para una adecuada y pertinente toma de decisiones basada en riesgos de seguridad de la información y en beneficio de reducir su impacto Alto o aprovechar la oportunidad.

c. TRATAMIENTO DE LOS RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Como resultado de la etapa de evaluación del riesgo tendremos una lista ordenada de riesgos o una matriz con la identificación de los niveles de riesgo de acuerdo con la zona de ubicación, por tanto, se deberá elegir la(s) estrategia(s) de tratamiento del riesgo en virtud de su valoración y de los criterios establecidos en el contexto de gestión de riesgos.

Basado en el nivel evaluación de los riesgos, se deberá seleccionar la opción de tratamiento adecuada por cada uno de los riesgos identificados; el costo/beneficio del tratamiento deberá ser un factor de decisión importante para la decisión.

De acuerdo a las análisis de costo/beneficio se sugiere como guía las siguientes opciones de tratamiento

COSTO – BENEFICIO	OPCION DE TRATAMIENTO
El nivel de riesgo está muy alejado del nivel de tolerancia, su costo y tiempo del tratamiento es muy superior a los beneficios	**Evitar** el riesgo, su propósito es no proceder con la actividad o la acción que da origen al riesgo (ejemplo, dejando de realizar una actividad, tomar otra alternativa, etc.)
El costo del tratamiento por parte de terceros (internos o externos) es más beneficioso que el tratamiento directo	**Transferir o compartir** el riesgo, entregando la gestión del riesgo a un tercero (ejemplo, contratando un seguro o subcontratando el servicio).
El costo y el tiempo del tratamiento es adecuado a los beneficios	**Reducir o Mitigar** el riesgo, seleccionando e implementando los controles o medidas adecuadas que logren que se reduzca la posibilidad o el impacto
La implementación de medidas de control adicionales no generará valor agregado para reducir niveles de ocurrencia o de impacto.	**Retener o acepta**r el riesgo, no se tomará la decisión de implementar medidas de control adicionales. Monitorizarlo para confirmar que no se incrementa

Tabla 7. Tratamiento de los riesgos de seguridad y privacidad de la información

El resultado de esta fase se concreta en un plan de tratamiento de riesgos, es decir, la selección y justificación de una o varias opciones para cada riesgo identificado, que permitan establecer la relación de riesgos residuales, es decir, aquellos que aún siguen existiendo a pesar de las medidas tomadas. Se recomienda ver la 27001 para la definición de controles

7. COMUNICACIÓN Y CONSULTA

Una vez finalizada la etapa de valoración y tratamiento de los riesgos y oportunidades se debe socializar con las partes involucradas para que conozcan de manera integral el estado de seguridad y privacidad de información y se tomen decisiones y se definan los planes de tratamiento.

8. MONITOREO Y SEGUIMIENTO DE LOS RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Periódicamente se revisará el valor de los activos, impactos, amenazas, vulnerabilidades y probabilidades en busca de posibles cambios, que exijan la valoración iterativa de los riesgos de seguridad de la información.

Los riesgos son dinámicos como la misma institución por tanto podrá cambiar de forma o manera radical sin previo aviso. Por ello es necesaria una supervisión continua que detecte: (1) nuevos activos o modificaciones en el valor de los activos,

(2) nuevas amenazas, (3) cambios o aparición de nuevas vulnerabilidades, (4) aumento de las consecuencias o impactos, (5) incidentes de seguridad de la información.

Con el propósito de conocer los estados de cumplimiento de los objetivos de la gestión de los riesgos de seguridad de la información, se deberán definir esquemas de seguimiento y medición al sistema de gestión de riesgos de la seguridad de la información que permitan contextualizar una toma de decisiones de manera oportuna.

9. PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

El Plan de Tratamiento de Riesgos contempla la definición de las actividades a desarrollar en aras de mitigar los riesgos sobre los activos y aprovechar las oportunidades, 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:

Gestión	Actividad	Tarea	Responsable	Fecha Inicio	Fecha Fin
Gestión de Riesgos	Actualización de lineamientos de riesgos	Actualizar política y metodología de gestión de riesgos	Grupo de Seguridad de la Información	02/2021	04/2021
	Sensibilización	Socialización Guía y Herramienta - Gestión de Riesgos de Seguridad y Privacidad de la Información	Grupo de Seguridad de la Información	02/2021	04/2021
	Identificación de Riesgos de la Seguridad y Privacidad de la Información	Identificación, Análisis y Evaluación de Riesgos -Seguridad y Privacidad de la Información	Grupo de Seguridad de la Información	01/2021	12/2021
		Realimentación, revisión y verificación de los riesgos identificados (ajustes)	Grupo de Seguridad de la Información	01/2021	12/2021
	Aceptación de los Riesgos Identificados	Aceptación, aprobación de Riesgos identificados y planes de tratamiento	Grupo de Seguridad de la Información- Comité de Seguridad de la Información	02/2021	12/2021

Gestión	Actividad	Tarea	Responsable	Fecha Inicio	Fecha Fin
	Socialización a las partes interesadas	Socialización Matriz de Riesgos	Grupo de Seguridad de la Información	03/2021	05/2021
	Seguimiento Fase de Tratamiento	Seguimiento estado planes de tratamiento de riesgos identificados y verificación de evidencias	Calidad	01/2021	12/2021
	Evaluación de riesgos residuales	Evaluación de riesgos residuales	Calidad – Control interno	01/2021	12/2021
	Mejoramiento	Identificación de oportunidades de mejoras acorde a los resultados obtenidos durante la evaluación de riesgos residuales.	Calidad- Grupo de Seguridad de la Información	01/2021	12/2021
		Actualización de la guía de Gestión de Riesgos Seguridad de la Información, de acuerdo a los cambios solicitados	Comité de seguridad de la Información	01/2021	12/2021
	Monitoreo y Revisión	Generación, presentación y reporte de indicadores	Oficial de Seguridad de la Información	01/2021	12/2021

Tabla 8. Plan de tratamiento de los riesgos de seguridad y privacidad de la información

10. RESPONSABLE DEL DOCUMENTO

Responsable de Seguridad de la Información y Oficial de Protección de Datos Personales.

11. TERMINOS Y DEFINICIONES

Administración del riesgo: Conjunto de elementos de control que al Interrelacionarse brindan a la entidad la capacidad para emprender las acciones necesarias que le permitan el manejo de los eventos que puedan afectar negativamente el logro de los objetivos institucionales y protegerla de los efectos ocasionados por su ocurrencia.

Activo de Información: En relación con la seguridad de la información, se refiere a cualquier información o elemento de valor para los procesos de la Organización.

Análisis de riesgos: Es un método sistemático de recopilación, evaluación, registro y difusión de información necesaria para formular recomendaciones orientadas a la adopción de una posición o medidas en respuesta a un peligro determinado.

Amenaza: Es la causa potencial de una situación de incidente y no deseada por la organización

Causa: Son todo aquello que se pueda considerar fuente generadora de eventos (riesgos). Las fuentes generadoras o agentes generadores son las personas, los métodos, las herramientas, el entorno, lo económico, los insumos o materiales entre otros.

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

Consecuencia: Resultado de un evento que afecta los objetivos.

Criterios del riesgo: Términos de referencia frente a los cuales la importancia de un riesgo se evaluada.

Control: Medida que modifica el riesgo.

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

Evaluación de riesgos: Proceso de comparación de los resultados del análisis del riesgo con los criterios del riesgo, para determinar si el riesgo, su magnitud o ambos son aceptables o tolerables.

Evento: Un incidente o situación, que ocurre en un lugar particular durante un intervalo de tiempo específico.

Estimación del riesgo. Proceso para asignar valores a la probabilidad y las consecuencias de un riesgo.

Evitación del riesgo. Decisión de no involucrarse en una situación de riesgo o tomar acción para retirarse de dicha situación.

Factores de Riesgo: Situaciones, manifestaciones o características medibles u observables asociadas a un proceso que generan la presencia de riesgo o tienden a aumentar la exposición, pueden ser internos o externos a la entidad.

Gestión del riesgo: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo, se compone de la evaluación y el tratamiento de riesgos.

Identificación del riesgo. Proceso para encontrar, enumerar y caracterizar los elementos de riesgo.

Incidente de seguridad de la información: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información (Confidencialidad, Integridad y Disponibilidad).

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

Impacto. Cambio adverso en el nivel de los objetivos del negocio logrados.

Nivel de riesgo: Magnitud de un riesgo o de una combinación de riesgos, expresada en términos de la combinación de las consecuencias y su posibilidad.

Matriz de riesgos: Instrumento utilizado para ubicar los riesgos en una determinada zona de riesgo según la calificación cualitativa de la probabilidad de ocurrencia y del impacto de un riesgo.

Monitoreo: Mesa de trabajo anual, la cual tiene como finalidad, revisar, actualizar o redefinir los riesgos de seguridad de la información en cada uno de los procesos, partiendo del resultado de los seguimientos y/o hallazgos de los entes de con trol o las diferentes auditorías de los sistemas integrados de gestión.

Propietario del riesgo: Persona o entidad con la responsabilidad de rendir cuentas y la autoridad para gestionar un riesgo.

Proceso: Conjunto de actividades interrelacionadas o que interactúan para transformar una entrada en salida.

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

Riesgo Residual: El riesgo que permanece tras el tratamiento del riesgo o nivel resultante del riesgo después de aplicar los controles.

Riesgo: Efecto de la incertidumbre sobre los objetivos.

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.

Reducción del riesgo. Acciones que se toman para disminuir la probabilidad las consecuencias negativas, o ambas, asociadas con un riesgo.

Retención del riesgo. Aceptación de la pérdida o ganancia proveniente de un riesgo particular

Seguimiento: Mesa de trabajo semestral, en el cual se revisa el cumplimiento del plan de acción, indicadores y metas de riesgo y se valida la aplicación de los controles de seguridad de la información sobre cada uno de los procesos.

Tratamiento del Riesgo: Proceso para modificar el riesgo" (Icontec Internacional, 2011).

Transferencia del riesgo. Compartir con otra de las partes la pérdida o la ganancia de un riesgo.

Valoración del Riesgo: Proceso global de identificación del riesgo, análisis del riesgo y evaluación de los riesgos.

Vulnerabilidad: Es aquella debilidad de un activo o grupo de activos de información

Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información.

SGSI: Sistema de Gestión de Seguridad de la Información.