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

UNIVERSIDAD DE LOS LLANOS
OFICINA DE SISTEMAS
VILLAVICENCIO, META
2021

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

1 INTRODUCCIÓN

1.1 Propósito del documento

La información durante los últimos años ha tomado una gran relevancia al interior de la entidades sobre todo cuando son públicas, no por la necesidad de acceder a ella veloz mente, sino asegurar que la información sea lo más confiable e integra posible para la toma de decisiones estratégicas o de desarrollo de la misión de las entidades, por esta razón el siguiente documento presenta el plan de tratamiento de riesgos de seguridad y privacidad de la Universidad de los Llanos, en el que se presenta proceso, etapas, metodología a utilizar, criterios para la identificación de los riesgos y el respectivo tratamiento como lo indica la norma ISO/IEC 27005.

1.2 Objetivo

Presentar el instrumento que expone las tareas necesarias para el respectivo tratamiento de los riesgos de seguridad y privacidad que tiene la información a la que accede y concentra la Unillanos a través de sus procesos institucionales.

1.3 Visión general del documento

El presente documento contiene los siguientes capítulos:

Capítulo 1 (Introducción): Presenta el propósito, la visión general y definiciones importantes para el entendimiento del documento.

Capítulo 2 (Visión general de la gestión del riesgo): Presenta una contextualización de la gestión del riesgo y la metodología a utilizar.

Capítulo 3 (Establecimiento de contexto): Presenta los criterios de evaluación de riesgos, impacto, de aceptación del riesgo y el alcance y límites para la gestión del riesgo.

Capítulo 4 (Valoración del riesgo): Presenta el análisis y evaluación del riesgo con la identificación y estimación del riesgo.

Capítulo 5 (Plan de tratamiento de riesgos de seguridad y privacidad de la información): Presenta la estrategia para el tratamiento de riesgos, recursos y el plan de tratamiento de riesgos.

Capítulo 6 (Anexos): Presenta los anexos relacionados con el plan de tratamiento de riesgos.

1.4 Definiciones, acrónimos y abreviaturas

1.4.1 Definiciones

- Criterio: Regla o norma conforme a lo establecido.
- 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.
- Identificación del riesgo: Proceso para encontrar, enumerar y caracterizar los elementos de riesgo.
- Impacto: Efecto positivo o negativo, resultado y/o consecuencias de la materialización de un riesgo.
- ISO/IEC 27005: Norma de gestión de seguridad de la información y la tecnología de las comunicaciones.
- NTC-ISO/IEC 27002: Estándar para la seguridad de la información que ha publicado la organización internacional de normalización.
- Probabilidad: Posibilidad de que suceda un fenómeno o hecho.
- Reducción del riesgo: Acciones que se toman para disminuir la probabilidad de las consecuencias, sin que suponga un perjuicio demasiado grave en los diferentes niveles institucionales.
- Retención del riesgo: Aceptación de las consecuencias provenientes de un riesgo particular, por la imposibilidad de efectuar controles; pero, que no afectan los criterios o políticas institucionales.
- Riesgos 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.
- Riesgo residual: Riesgo que permanece después de la implementación de controles.
- Transferencia del riesgo: Compartir con otras partes la pérdida o la ganancia de un riesgo.
- Valoración: Proceso que consiste de calcular valor del riesgo en este caso en particular.

1.4.2 Acrónimos

Tabla 1. Acrónimos

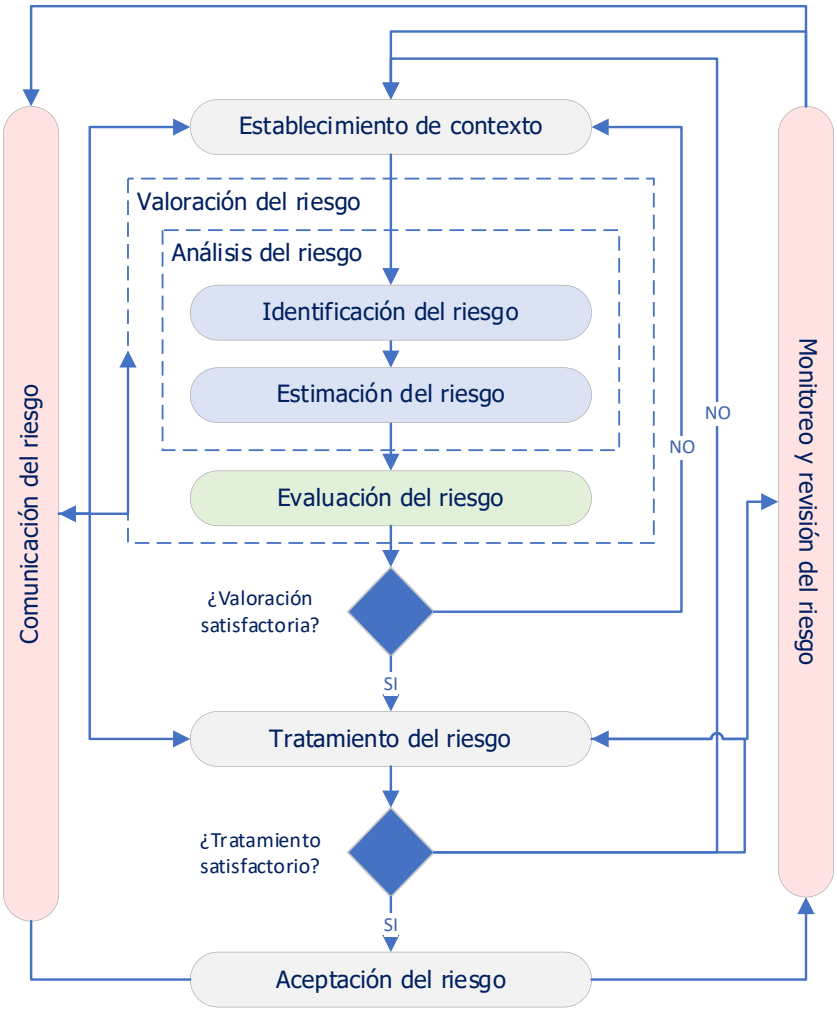
Acrónimo	Descripción
NTC	Norma Técnica Colombiana
ISO	International Organization for Standardization (Organización Internacional de Normalización)
IEC	International Electrotechnical Commission (Comisión Electrotécnica Internacional)

2 VISIÓN GENERAL DE LA GESTIÓN DEL RIESGO

2.1 Contextualización

La gestión del riesgo permite a través de diferentes acciones proteger la información, sistemas de información y activos de una entidad y/o institución, ya que por medio de esta se pueden implementar controles de seguridad de acuerdo a las vulnerabilidades que deben ser identificadas en los diferentes procesos institucionales, la norma ISO/IEC 27005 presenta una visión del proceso de gestión de riesgos que se planteará para la Universidad de los Llanos, ver Figura 1.

Figura 1. Proceso de gestión de riesgos de seguridad de la información (ISO/IEC 27005)



Como se observa en la Figura 1, el proceso de gestión del riesgo debe ser iterativo ya que los riesgos pueden ir cambiando o simplemente para asegurar las medidas propuestas a mitigar los riesgos.

Con lo anterior se podría resumir las actividades del proceso de gestión de riesgos de seguridad de la información en 4 etapas, estas se exponen en la Tabla 2.

Tabla 2. Etapas gestión del cambio

Etapa	Actividades
Planear	Establecer contexto.
	Valoración del riesgo.
	Planificación del tratamiento del riesgo.
	Aceptación del tratamiento.
Hacer	Implementación del plan de tratamiento del riesgo.
Verificar	Monitoreo y revisión del plan de tratamiento del riesgo.
Actuar	Mantener y mejorar el proceso de gestión del riesgo en la seguridad de la información.

2.1.1 Establecer contexto

Establecer los criterios básicos necesarios para la gestión del riesgo de seguridad de la información, alcance, organizacional para desarrollar el proceso.

- Criterios de evaluación: Se debe definir los criterios de evaluación con los que se realizará el plan de riesgos.
- Criterios de impacto: Se debe definir criterios de impacto del riesgo y clasificarlos en términos del grado del daño o costos para la institución.
- Criterios de aceptación del riesgo: Se debe especificar criterios de aceptación del riesgo que dependerán de las políticas, metas y objetivos de la institución, estos niveles pueden tener umbrales, pueden incluir un requisito para un tratamiento futuro y pueden tener expectativa de duración.
- Alcance y límites para la gestión del riesgo en seguridad de la información: Se debe definir el alcance y los límites de la gestión del riesgo, con el fin de definir activos, interesados y procesos identificados.
- Organización para la gestión del riesgo: Se debe asignar un responsable(s) del proceso de gestión del riesgo de seguridad de la información y definir responsabilidades.

2.1.2 Valoración del riesgo

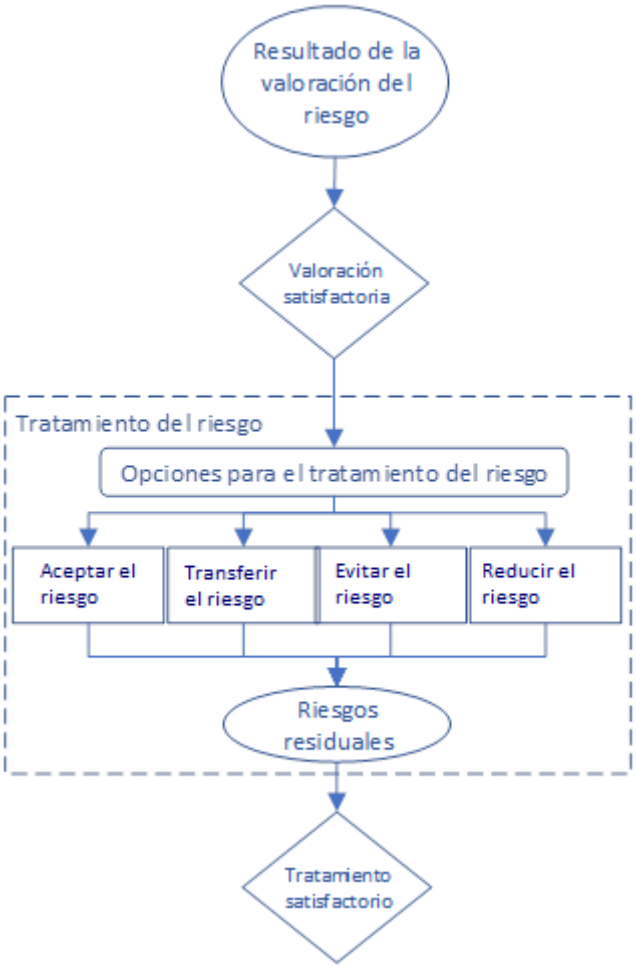
Dentro de la valoración del riesgo se debe identificar, describir y priorizar los riesgos de acuerdo a los criterios definidos anteriormente, para esto se tienen actividades importantes como:

- Análisis del riesgo, el análisis consta de:
  - Identificación del riesgo: Identificar los riesgos de acuerdo al alcance (Identificación de activos, identificación de amenazas, identificación de controles existentes, identificación de vulnerabilidades, identificación de consecuencias)
  - Estimación del riesgo: La estimación puede ser cualitativa, cuantitativa o una combinación de ambas, que dependerá totalmente de la criticidad de los activos, vulnerabilidades e incidentes que han pasado anteriormente, se debe evaluar el impacto al negocio o consecuencias de los riesgos, valoración de los incidentes y estimar el nivel del riesgo para los diferentes escenarios de incidentes pertinentes.
- Evaluación del riesgo: Se deben comparar los niveles de riesgos frente a los criterios de evaluación y aceptación.

2.1.3 Tratamiento del riesgo

Se deben definir controles para aceptar, transferir, evitar o reducir, todo por medio del plan de tratamiento de riesgos, el tratamiento se puede representar en la Figura 2, a continuación, una representación gráfica de la actividad de tratamiento de riesgos.

Figura 2. Actividades del tratamiento de riesgos



Como se observa en la figura anterior como insumo para el tratamiento de los riesgos se requiere el resultado de la valoración del riesgo, con los respectivos análisis, estimaciones y evaluaciones de riesgos.

2.1.4 Aceptación del riesgo

En la aceptación del riesgo de acuerdo al plan de tratamiento y la valoración del riesgo residual, se debe hacer un análisis para la aceptación de los riesgos y las responsabilidades de las decisiones, obteniendo como resultado una lista de los riesgos aceptados con su respectiva justificación.

2.1.5 Comunicación de los riesgos de la seguridad de la información

Se debe comunicar a los diferentes interesados o personas involucradas en la institución la información relacionada a los riesgos desde cualquier etapa, con el fin de llegar a acuerdos para la gestión de los mismos.

2.1.6 Monitoreo y revisión del riesgo en la seguridad de la información

Esta actividad parte de la necesidad de monitorear y revisar los riesgos de forma continua ya que estos no son estáticos, sino que pueden tener cambios y presentarse nuevas amenazas o vulnerabilidades.

2.2 Metodología

De acuerdo al Marco de seguridad y privacidad de la información, el plan de tratamiento de riesgos requiere de un conjunto de actividades insumo que se deben asegurar para poder trazar de forma correcta un plan y poder mitigar los riesgos de la institución, de acuerdo con lo anterior la metodología a implementar requiere la ejecución de las siguientes actividades:

- Conocimiento, actualización o definición de las políticas de seguridad de la información.
- Levantamiento y diagnostico con líderes de procesos.
- Definición o actualización de los criterios para identificación de riesgos.
- Identificación y análisis de riesgos de seguridad de la información.
- Estimación de riesgos de seguridad de la información.
- Evaluación de riesgos de seguridad de la información.
- Identificar métodos de tratamiento.
- Elaborar plan de tratamiento de riesgos de seguridad de la información.

3 ESTABLECIMIENTO DE CONTEXTO

Para la definición del plan de tratamiento de riesgos de seguridad y privacidad de la información se definen los criterios básicos (de acuerdo a la norma) necesarios para el ejercicio de identificación de riesgos, vulnerabilidades y demás, a continuación, los criterios:

3.1 Criterios de evaluación de riesgos

La evaluación de los riesgos debe tener en cuenta los siguientes aspectos:

- Requisitos legales, reglamentarios y obligaciones contractuales.
- Criticidad de los activos de información involucrados desde cada proceso institucional.
- Importancia de la disponibilidad, confidencialidad e integridad de la información para las operaciones.
- Expectativas y percepciones de las partes interesadas y consecuencias negativas que involucren la reputación de la institución.

3.2 Criterios de impacto

Los criterios de impacto que se consideran son los siguientes:

- Daños para la reputación e imagen institucional.
- Operaciones deterioradas.
- Alteración de planes y fechas límites.
- Incumplimiento de objetivos estratégicos.
- Incumplimiento de los requisitos legales.
- Afectación financiera.
- Brechas en la seguridad de la información (Perdida de confidencialidad, integridad y disponibilidad).

3.3 Criterios de aceptación del riesgo

Los criterios de aceptación del riesgo considerados son los siguientes:

- Pueden incluir umbrales múltiples, con una meta de nivel de riesgo deseable, pero disposiciones para que la alta dirección acepte los riesgos encima de este nivel.
- Expresar como la relación entre el beneficio estimado y el riesgo estimado.
- Se puede aplicar a riesgos que podrían resultar en incumplimiento con reglamentos o leyes, en caso de que se especifique en un requisito contractual.
- Los criterios pueden incluir tratamiento adicional en el futuro.
- Los criterios pueden diferir de acuerdo con la expectativa de duración que tenga el riesgo.

3.4 Alcance y límites para la gestión del riesgo en seguridad de la información

El alcance para el desarrollo e implementación de la gestión de los riesgos de seguridad y privacidad de la información y el respectivo tratamiento de esos riesgos se basan en los procesos institucionales y la prioridad que se le den en la institución y por supuesto al tratamiento de los riesgos valorados como externos, debido a su urgencia en el tratamiento.

4 VALORACIÓN DEL RIESGO

Un insumo importante para realizar la valoración del riesgo de los riesgos de seguridad y privacidad de la información es el inventario de los activos de información, entrevistas con los interesados de los diferentes procesos institucionales.

Para el desarrollo del inventario ver anexo 1.

4.1 Análisis del riesgo

4.1.1 Identificación del riesgo

Todo inicia con la identificación de los riesgos de seguridad y privacidad de la información y esta se realizará como indicamos con anterioridad por medio de los activos de información que se clasificarán de la siguiente manera:

4.1.1.1 Primarios

- Procesos: En procesos con importancia alta, que su cumplimiento afecte la misión de la institución.
- Información: Información vital, estratégica y de alto costo en recolección, almacenamiento, procesamiento y transmisión.

4.1.1.2 Soporte

- Hardware: Elementos físicos que soportan los procesos.
- Software: Software que aportan en el procesamiento de la información.
- Redes: Dispositivos de infraestructura tecnológica que permite la conexión entre los dispositivos y sistemas de información.
- Personal: Recurso humano relacionados con el software.
- Sitio: Ubicación física.
- Estructura organizacional: Recurso humano responsable que hacen parte de áreas, dependencias.

Dentro de la identificación de los riesgos se debe identificar las amenazas que pueden causar daños en la información, en los procesos y los soportes, así mismo analizar vulnerabilidades.

4.1.2 Estimación del riesgo

Para la estimación de los riesgos se contempla establecer esa probabilidad de que pasen y el impacto de las consecuencias, para esto se van a definir las siguientes escalas:

4.1.2.1 Probabilidad

Posibilidad de que acontezca el riesgo.

Tabla 3. Niveles de probabilidad

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

4.1.2.2 Impacto

Para ver las consecuencias por materialización del riesgo, ver la Tabla 4.

Tabla 4. Valor de impacto

Ítem	Nivel	Afectación económica	Reputacional
1	Insignificante	Afectación menor a 10 SMLMV	El riesgo afecta la imagen de algún área de la organización.
2	Menor	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
3	Moderado	Entre 50 y 100 SMLMV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos.
4	Mayor	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.
5	Catastrófico	Mayor a 500 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país.

4.2 Evaluación del riesgo

Ahora de acuerdo a las categorías definidas para los niveles de probabilidad y los impactos de materialización de los riesgos se inicia un análisis y evaluación que permitirá evidenciar la criticidad de tratamiento de los riesgos identificados anteriormente.

Tabla 5. Matriz de evaluación del riesgo

Probabilidad	Muy Alta 100%	Alto	Alto	Alto	Alto	Extremo
	Alta 80%	Moderado	Moderado	Alto	Alto	Extremo
	Media 60%	Moderado	Moderado	Moderado	Alto	Extremo
	Baja 40%	Bajo	Moderado	Moderado	Alto	Extremo
	Muy Baja 20%	Bajo	Bajo	Moderado	Alto	Extremo
		Leve 20%	Menor 40%	Moderado 60%	Mayor 80%	Catastrófico 100%
		Impacto				

Con la matriz de la Tabla 5 se pueden identificar la exposición o zonas de riesgos de las entidades según la probabilidad del impacto y permite tomar decisiones para la priorización en el tratamiento de los riesgos identificados, las zonas de riesgo son las siguientes:

- Riesgos Baja: Zona de color verde.
- Riesgo moderado: Zona de color amarillo.
- Riesgo alto: Zona de color rosa.
- Riesgo extremo: Zona de color rojo.

Para evaluar el riesgo ver anexo 2.

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

5.1 Metodología

Con el fin de ejecutar de la mejor forma el plan de tratamiento de riesgos de seguridad y privacidad de la información se define una metodología que dependerá de las acciones o fases que requiera ejecución, las fases son las siguientes:

5.1.1 Fase 1 (Planeación)

- Descripción: Fase actual que permite realizar el análisis e identificación de actividades mínimas a ejecutar, alcance, tiempos y responsables, para el inicio del tratamiento de los riesgos.
- Responsable: Equipo de trabajo de seguridad y privacidad de la información (Oficina de sistemas).

5.1.2 Fase 2 (Levantamiento y análisis de información)

- Descripción: Esta fase recoge diferentes actividades entre ellas se encuentra la capacitación en valoración de activos e identificación de riesgos a los líderes o responsables de los procesos institucionales, el respectivo análisis de la información resultado posterior de las capacitaciones y su documentación por medio de la matriz de riesgos.
- Responsable: Líderes y/o responsables de procesos institucionales y equipo de trabajo de seguridad y privacidad de la información (Oficina de sistemas).

5.1.3 Fase 3 (Establecimiento de controles)

- Descripción: La fase tres permitirá definir los controles y su relación de mitigación a los riesgos identificados y por último priorización de los controles de acuerdo a la evaluación de impacto/probabilidad, ya que la ejecución depende del compromiso no solo directivo sino de los diferentes líderes de procesos.
- Responsable: Líderes y/o responsables de procesos institucionales y equipo de trabajo de seguridad y privacidad de la información (Oficina de sistemas).

5.1.4 Fase 4 (Ejecución)

- Descripción: La fase de ejecución iniciara con el desarrollo de los diferentes controles establecidos para la mitigación de los riesgos, por medio de diferentes acciones, sensibilizaciones, capacitaciones, planteamiento y ejecución de proyectos entre otros.
- Responsable: Líderes y/o responsables de procesos institucionales y equipo de trabajo de seguridad y privacidad de la información (Oficina de sistemas).

5.1.5 Fase 5 (Monitoreo)

- Descripción: Se debe realizará seguimiento a los líderes de los procesos, de acuerdo a las actividades planteadas en el cronograma de trabajo, mínimo 1 vez por semestre o de acuerdo a la necesidad de los líderes de proceso.
- Responsable: Equipo de trabajo de seguridad y privacidad de la información (Oficina de sistemas).

5.2 Estrategia en el tratamiento de riesgos

El objetivo principal de la estrategia para el tratamiento de riesgos es minimizarla probabilidad de materialización del riesgo a través de cuatro opciones de tratamiento:

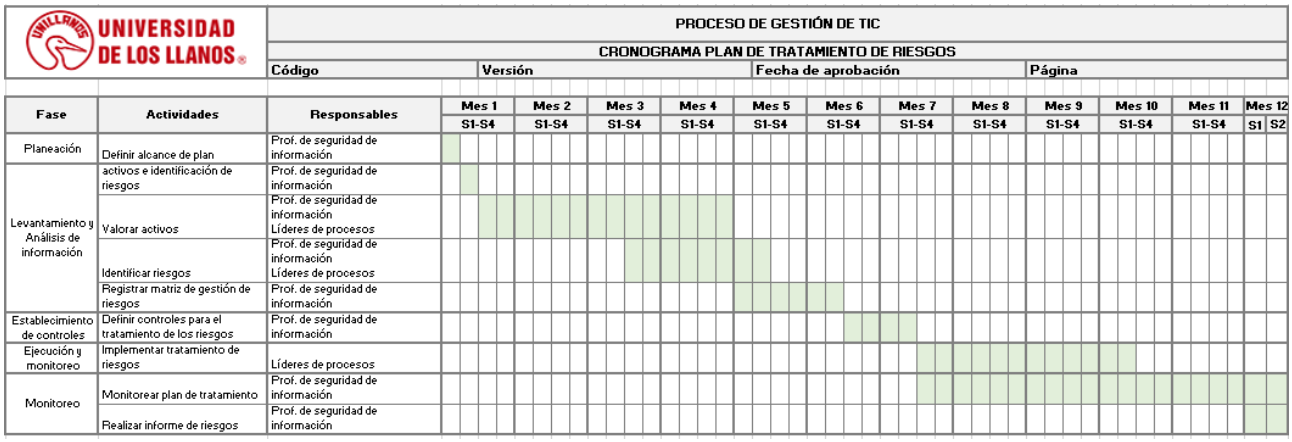
- Reducción del riesgo: La finalidad de la reducción de los riesgos es la mitigación del riesgo residual y se pueda reevaluar como aceptable por medio de la implementación de controles (Controles definidos en la NTC-ISO/IEC 27002).
- Aceptación del riesgo: La aceptación consiste en la aceptación del riesgo debido a la imposibilidad de implementar controles adicionales, pero satisfacen los diferentes criterios y políticas institucionales.
- Evitación del riesgo: La metodología a utilizar es la de evitar las actividades que incorporan los riesgos o transformar las actividades que cumplan con el mismo objetivo pero que no incluyan el riesgo detectado.
- Transferencia del riesgo: Esta opción de tratamiento de los riesgos permite trasladar el riesgo a otra parte (Tercero) que pueda gestionarlo de manera eficaz.

5.3 Recursos

Humano: Líderes de procesos y profesional de seguridad de la información.
Físicos: Equipos de cómputo, servidores y equipos de red.
Financieros: Disponibilidad de recursos para estas tareas.

5.4 Cronograma

Figura 3. Cronograma de plan de tratamiento de riesgos



UNIVERSIDAD DE LOS LLANOS

PROCESO DE GESTIÓN DE TIC

CRONOGRAMA PLAN DE TRATAMIENTO DE RIESGOS

Código	Versión	Fecha de aprobación	Página

Fase	Actividades	Responsables	Mes 1	Mes 2	Mes 3	Mes 4	Mes 5	Mes 6	Mes 7	Mes 8	Mes 9	Mes 10	Mes 11	Mes 12
			S1-S4	S1-S4	S1-S4	S1-S4	S1-S4	S1-S4	S1-S4	S1-S4	S1-S4	S1-S4	S1-S4	S1 S2
Planeación	Definir alcance de plan	Prof. de seguridad de información												
Levantamiento y Análisis de información	activos e identificación de riesgos	Prof. de seguridad de información												
	Valorar activos	Prof. de seguridad de información Líderes de procesos												
	Identificar riesgos	Prof. de seguridad de información Líderes de procesos												
	Registrar matriz de gestión de riesgos	Prof. de seguridad de información												
Establecimiento de controles	Definir controles para el tratamiento de los riesgos	Prof. de seguridad de información												
Ejecución y monitoreo	Implementar tratamiento de riesgos	Líderes de procesos												
Monitoreo	Monitorear plan de tratamiento	Prof. de seguridad de información												
	Realizar informe de riesgos	Prof. de seguridad de información												

Para un mayor detalle ver anexo 3.

6 Historial de cambios

Versión	Fecha	Cambios	Elaboró / Modificó	Revisó	Aprobó
01	15/12/2021	Documento nuevo	Andrea Pinilla *Prof. Apoyo Oficina de Sistemas*	Armando Garzón *Jefe Oficina de Sistemas*	Armando Garzón *Jefe Oficina de Sistemas*

7 ANEXOS

Anexo 1. FO-GRT-06 Formato inventario de activos de información

Anexo 2. FO-GRT-07 Formato matriz de riesgos de seguridad y privacidad de la información

Anexo 3. Cronograma plan de tratamiento de riesgos