PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

OFICINA DE SISTEMAS

2025

CONTENIDO

Introducción 3
1. Objeto 3
2. Alcance 3
3. Referencias Normativas 3
4. Definiciones 3
5. Condiciones Generales 4
6. Contenido 4
   6.1 Metodología Gestión De Riesgos 4
   6.2 Cronograma 5
   6.3 Recursos 6
7. Flujograma 6
8. Listado De Anexos 6
9. Historial De Cambios 6

INTRODUCCIÓN

Este plan describe un enfoque claro y estructurado del proceso para realizar la identificación, valoración, y tratamiento de los riesgos de seguridad sobre los activos de información de la Universidad alineado con la política de gestión integral del riesgo, con el fin de preservar la seguridad e integridad de los activos; de acuerdo a lo establecido en la guía para la administración del riesgo y el diseño de controles en entidades públicas emitida por el DAFP.

1. OBJETO

Definir las actividades necesarias para el proceso de identificación de los riesgos de seguridad de la información asociados a los activos de información en cada uno de los procesos de la Universidad, así como de las posibles acciones para mitigarlos de manera preventiva e integral, contribuyendo así a protección de la integridad, confidencialidad y disponibilidad de la información.

2. ALCANCE

El alcance del presente plan es aplicable para la identificación y gestión de los riesgos de seguridad de la información de los activos de información en la Universidad de los Llanos.

3. REFERENCIAS NORMATIVAS

- **Decreto 1078 de 2015.** Por medio del cual se expide el decreto único reglamentario del sector de las tecnologías de la información y las comunicaciones.
- **Decreto 1008 de 2018**. Por el cual se establecen los lineamientos generales de la política de Gobierno Digital.
- **Norma Técnica Colombiana NTC-ISO/IEC 27005** Tecnología de la Información. Técnicas de Seguridad. Gestión del Riesgo en la Seguridad de la Información.
- **Guía para la administración del riesgo y el diseño de controles en entidades públicas- 2022 – Versión 6** -DAFP.
- **Acuerdo Superior 012 de 2020,** *"Por el cual se adopta la Política para la Gestión Integral de Riesgos en la Universidad de los Llanos".*
- **Resolución 500 de 2021**. Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital.
- **Resolución 746 de 2022.** Por la cual se fortalece el modelo de seguridad y privacidad de la información y se definen lineamientos adicionales a los establecidos en la resolución No. 500 de 2021.
- **Decreto 767 de 2022.** Actualización Política de Gobierno Digital.

4. DEFINICIONES

- **Activo:** Cualquier recurso de la empresa necesario para desempeñar las actividades diarias. La valoración de los activos es importante para la evaluación de la magnitud del riesgo
- **Amenaza:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.
- **Confidencialidad:** Propiedad que determina la condición de que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.
- **Consecuencia**: los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas.

- **Control:** Medida que permite reducir o mitigar un riesgo.
- **Criterio**: Regla o norma conforme a la cual se establece un juicio o se toma una determinación.
- **Estimación del riesgo**: Proceso para asignar valores a la probabilidad y las consecuencias de un riesgo.
- **Evento**: Posible ocurrencia de Incidente o amenaza de Seguridad de la Información.
- **Identificación del riesgo**: Se determinan las causas, fuentes del riesgo y los eventos con base al contexto el proceso, que pueden afectar el logro de los objetivos del mismo.
- **Impacto:** Efecto positivo o negativo, resultado y/o consecuencias de la materialización de un riesgo.
- **ISO/IEC 27005**: Es el estándar internacional que se ocupa de la gestión de riesgos de seguridad de la información en una empresa.
- **Probabilidad:** Es la posibilidad de ocurrencia de un hecho, suceso o acontecimiento.
- **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.
- **Riesgo de Corrupción**: Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.
- **Riesgo Inherente:** Se refiere al riesgo identificado inicialmente sin aplicar ninguna medida de tratamiento.
- **Riesgo residual**: Riesgo que permanece después de la implementación de controles.
- **Riesgo:** Es la probabilidad de que ocurra un evento y una amenaza se materialice causando efectos negativos.
- **Transferencia del riesgo**: Compartir con otras partes la pérdida o la ganancia de un riesgo.
- **Vulnerabilidad:** Representa la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.

5. CONDICIONES GENERALES

No aplica

6. CONTENIDO

6.1 Metodología Gestión de Riesgos

El proceso para la gestión de riesgos de seguridad de la información en la Universidad de los Llanos, se realizará acorde con la metodología descrita en el **procedimiento "*PD-DIE-03 - Gestión de los Riesgos y Oportunidades Institucionales***, la cual debe cumplir con lo establecido en la *"Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas"* emitida por el Departamento Administrativo de Función Pública-DAFP" y el modelo de gestión de riesgos descrito en el anexo 4 *"Modelo Nacional de Gestión de Riesgo de seguridad de la Información en Entidades Públicas"* en su versión vigente. Así se garantiza que los riesgos de seguridad de la información sean identificados, evaluados y gestionados de manera integral, con un enfoque que promueve la mejora continua y la adaptación a los cambiantes entornos tecnológicos y de seguridad digital.

El proceso para la gestión de los riesgos de seguridad de la información se compone de las siguientes etapas:

a) **Identificación de los riesgos** En esta etapa se deben identificar los riesgos que pueden impactar sobre la seguridad de los activos más importantes (hardware, software, documentos, servicios, personas, etc.) y que deben ser protegidos para garantizar su funcionamiento.

b) **Evaluación de riesgos** Una vez que los riesgos han sido identificados, se procede a evaluar tanto la probabilidad de ocurrencia de cada riesgo como el impacto potencial que tendría en caso de materializarse. La evaluación se lleva a cabo utilizando los criterios de valoración de riesgos

previamente establecidos, lo que facilita la priorización de los riesgos y la toma de decisiones fundamentadas sobre las acciones a seguir para su tratamiento.

c) Tratamiento de riesgos Una vez analizados y evaluados los riesgos, se deben definir estrategias para su tratamiento.

A la hora de evaluar las opciones existentes en materia de tratamiento del riesgo, los dueños de los procesos tendrán en cuenta la importancia del riesgo, lo cual incluye el efecto que puede tener sobre la entidad, la probabilidad e impacto del riesgo, y la relación costo beneficio de las medidas de tratamiento.

Para el tratamiento de cada uno de los riesgos analizados y evaluados la Política institucional define las siguientes estrategias para combatir el riesgo:

- **Aceptar**: Se trata de asumir el riesgo y las consecuencias que implican la materialización del mismo. Si el nivel de riesgo cumple con los criterios de aceptación de riesgo, no es necesario poner controles y el riesgo puede ser aceptado. Esto debería aplicar para riesgos inherentes en la zona de calificación de riesgo bajo.
- **Compartir o transferir**: Trasladar a un tercero ajeno al proceso la gestión del riesgo. Cuando es muy difícil para la entidad reducir el riesgo a un nivel aceptable, o se carece de conocimientos necesarios para gestionarlo, el riesgo puede ser compartido con otra parte interesada que pueda gestionarlo con más eficacia. Cabe señalar que normalmente no es posible transferir la responsabilidad del riesgo.
- **Evitar**: Cuando los escenarios de riesgo identificado se consideran demasiados extremos, se puede tomar una decisión para evitar el riesgo, mediante la cancelación de una actividad o conjunto de actividades.
- **Reducir**: Se espera disminuir el impacto de la materialización del riesgo, debilitando los efectos negativos. El nivel de riesgo debe ser administrado mediante el establecimiento de controles, de modo que el riesgo residual se pueda reevaluar como algo aceptable para la entidad. Estos controles disminuyen normalmente la probabilidad y/o el impacto del riesgo.

d) Monitoreo Esta fase incluye la supervisión de los controles establecidos e implementados, de acuerdo a la periodicidad establecida para asegurar que las estrategias de tratamiento de riesgos sigan siendo efectivas.

6.2 Cronograma

La oficina de sistemas apoyará el proceso de identificación de riesgos de seguridad de la información y el establecimiento de los controles a implementar con los líderes de cada uno de los procesos o dependencias. Los riesgos de seguridad de la información identificados se reflejarán en la matriz de riesgos dispuesta para ello, donde se establecerán las acciones de control y las fechas para implementar dichos controles.

Las actividades a ejecutar en el proceso para la gestión de los riesgos de seguridad de la información en la Universidad de los Llanos para la vigencia 2025 son las siguientes:

Tabla 1. Cronograma 2025

Fase	Actividades	Evidencias	Responsables	Fecha
Identificación y evaluación de riesgos	Consolidar la matriz de riesgos de seguridad de la información.	Matriz de riesgos consolidado	Prof. de seguridad de la información	
Aceptación de Riesgos Identificados	Aceptación y aprobación riesgos identificados y planes de tratamiento	Acta o correo de aprobación de riesgos.	Prof. de seguridad de la información Líderes de procesos	Febrero-marzo 205

Fase	Actividades	Evidencias	Responsables	Fecha
Publicación	Publicación matriz de riesgos de los procesos	Matriz de riesgos publicada /URL de publicación	Prof. de seguridad de la información Oficina SIG	Marzo 2025
Monitoreo y Revisión	Seguimiento implementación de controles y tratamiento establecido	Verificación de evidencias	Prof. de seguridad de la información Líderes de procesos Oficina de Control Interno	Abril-diciembre 2025
Tratamiento	Realizar las acciones de tratamiento de los riesgos identificados	Soportes de ejecución de las acciones	Líder proceso Gestión TIC / Profesional de seguridad de la información	Diciembre2025
Monitoreo y Revisión	Medición, presentación y reporte de indicadores	Matriz de riesgos	Prof. de seguridad de la información	
Identificación y evaluación de riesgos	Identificación de riesgos y establecimiento del plan de tratamiento para la siguiente vigencia		Prof. de seguridad de la información Líderes de procesos	Noviembre 2025
Identificación y evaluación de riesgos	Consolidar la matriz de riesgos de seguridad de la información.	Matriz de riesgos consolidado	Prof. de seguridad de la información	Diciembre 2025
Aceptación de Riesgos Identificados	Aceptación y aprobación riesgos identificados y planes de tratamiento	Acta o correo de aprobación de riesgos.	Prof. de seguridad de la información Líderes de procesos	Diciembre 2025

Fuente: Elaboración propia.

6.3 Recursos

El desarrollo de las actividades para lograr su consecución estará sujeto a la disponibilidad de recursos (humanos, técnicos, tecnológicos, financieros) que se requieran para el cumplimiento de las actividades; de acuerdo con la disponibilidad presupuestal oportuna, al apetito de riesgo institucional y a las orientaciones de la alta dirección.

7. FLUJOGRAMA

No aplica

8. LISTADO DE ANEXOS

Este documento no cuenta con anexos

9. HISTORIAL DE CAMBIOS

Versión	Fecha	Cambios	Elaboró/Modificó	Revisó	Aprobó
02	27/09/2022	Se reestructuró el documento y sus actividades.	Andrea Pinilla *Prof. Apoyo Oficina de Sistemas*	Armando Garzón *Jefe Oficina de Sistemas*	Armando Garzón *Jefe Oficina de Sistemas*
03	04/07/2024	Se actualizó el documento para la vigencia 2024.	Mónica Hernández *Prof. Seguridad de la Información*	Roiman A. Sastoque *Jefe Oficina de Sistemas*	Roiman A. Sastoque *Jefe Oficina de Sistemas*
04	18/02/2025	Se actualizaron las actividades del plan para la vigencia 2025.	Mónica Hernández *Prof. Seguridad de la Información*	Adriana Ramos *Prof. de apoyo de Planeación*	Roiman A. Sastoque *Jefe Oficina de Sistemas*