PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

OFICINA DE SISTEMAS

2026

CONTENIDO

1. INTRODUCCIÓN

El presente plan establece la metodología para la gestión de los riesgos de seguridad de la información asociados a los activos de información críticos de la Universidad, en concordancia con la Política de Gestión Integral del Riesgo y los lineamientos definidos por el Departamento Administrativo de la Función Pública, con el propósito de preservar la seguridad de la información institucional.

Así mismo, el plan contempla la identificación y clasificación de los activos de información, así como la identificación de riesgos, amenazas y vulnerabilidades, para realizar el análisis y evaluación de los riesgos de seguridad de la información. A partir de dicho análisis, se definen e implementan los controles necesarios para su tratamiento y mitigación, incluyendo el correspondiente proceso de seguimiento y reporte.

2. OBJETIVO

Establecer los elementos metodológicos para identificar, analizar, valorar y tratar los riesgos de seguridad, asociados a los activos de información críticos de cada uno de los procesos de la Universidad, con el fin de contribuir a la protección de la integridad, confidencialidad y disponibilidad de la información.

3. ALCANCE

Esta guía aplica para la gestión de los riesgos de seguridad de la información en todos los procesos de la Universidad, conforme a lo establecido en la Política para la Gestión Integral de Riesgos de la Universidad.

4. 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 gestión integral del riesgo en entidades públicas- 2025 – Versión 7** -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.

5. DEFINICIONES

- **Activo:** [Según ISO 27000]: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización.

- **Amenaza:** [Según ISO 27000]: 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:** [NTC ISO 31000:2011]: Resultado o impacto de un evento que afecta a los objetivos.

- **Controles:** [Según ISO 27000]: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido.

- **Dato Personal**: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.

- **Disponibilidad**: Propiedad que consiste en la accesibilidad y usabilidad de la información cuando se requiera por una entidad autorizada.

- **Evaluación del Riesgo:** [Según NTC ISO 31000:2011]: 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.

- **Impacto:** [Según ISO 27000]: El coste para la empresa de un incidente -de la escala que sea-, que puede o no ser medido en términos estrictamente financieros -p.ej., pérdida de reputación, implicaciones legales, etc.

- **Integridad**: Propiedad que consiste en la precisión y completitud de la información.

- **Probabilidad**: Es la posibilidad de ocurrencia del riesgo.

- **Riesgo:** Probabilidad de que una amenaza pueda explotar vulnerabilidades en los activos, comprometiendo la confidencialidad, integridad y disponibilidad de la información.

- **Riesgo Inherente**: Se refiere al riesgo identificado inicialmente sin aplicar ninguna medida de tratamiento.

- **Riesgo Residual:** Es el riesgo resultante después de aplicar uno o más controles.

- **Vulnerabilidad:** [Según ISO 27000]: Debilidad de un activo o control que puede ser explotada por una o más amenazas.

6. POLÍTICA DE GESTIÓN DE RIESGOS DE SEGURIDAD

La Universidad de los Llanos cuenta con la Política para la Gestión Integral de Riesgos, adoptada mediante el Acuerdo Superior No. 012 de 2020, la cual incorpora la gestión de los riesgos asociados a la seguridad digital.

7. RECURSOS PARA LA GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

La identificación de los recursos necesarios para la gestión de los riesgos de seguridad de la información estará a cargo de los líderes de proceso, o jefes de área con el apoyo del profesional de seguridad de la información. Estos requerimientos serán presentados a la alta dirección, quien priorizará su tratamiento según el impacto para la Universidad. El dueño del riesgo será responsable de la gestión de los recursos, así como del seguimiento, control e implementación del plan de tratamiento.

8. METODOLOGÍA DE GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

La Universidad de los Llanos adopta la metodología definida por el Departamento Administrativo de la Función Pública (DAFP), establecida en la "*Guía para la Gestión*

Integral del Riesgo en Entidades Públicas – Versión 7 (2025)" alineada con los "Lineamientos del Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas" del MinTIC, con el propósito de preservar la confidencialidad, integridad y disponibilidad de los activos de información institucionales.

Los riesgos de seguridad de la información se identifican, valoran y tratan de manera progresiva en la Matriz Institucional de Riesgos de Seguridad de la Información establecida para ello, la cual constituye el instrumento oficial para su registro, análisis, seguimiento y actualización.

El proceso para la identificación y tratamiento de los riesgos asociados con dichos activos de información se desarrolla a través de las siguientes fases:

8.1. FASE DE PLANIFICACIÓN:

a) Identificación y descripción de riesgos de seguridad de la información

Para la identificación de los riesgos de seguridad de la información, es necesario identificar previamente los activos de información asociados a cada proceso. Estos activos incluyen, entre otros: la información; el software (programas informáticos); el hardware (equipos de cómputo); los servicios; las personas y sus competencias, habilidades y experiencia; así como los activos intangibles, tales como la reputación y la imagen institucional.

La identificación y valoración de los activos de información se realizará de conformidad con los criterios establecidos por el MSPI en la Guía "Lineamientos del Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas". Con base en su nivel de criticidad, se determinarán los activos a los cuales se les efectuará el correspondiente análisis de riesgos. Dichos activos serán registrados en la Matriz Institucional de Riesgos de Seguridad de la Información establecida por la Universidad, considerando aspectos como su valor, responsables, ubicación y tipo de activo, entre otros.

Las Tablas de Retención Documental vigentes se utilizarán como fuente principal para la identificación de la información institucional. Los activos de información que no se encuentren contemplados en dichas tablas deberán ser identificados y documentados de manera complementaria por los responsables de los procesos, en coordinación con los jefes de área.

En esta etapa para cada activo de información identificado, se determinan los riesgos de seguridad de la información, considerando las **amenazas** potenciales y las **vulnerabilidades** asociadas, tanto técnicas como organizacionales, que puedan afectar la **confidencialidad**, **integridad** o **disponibilidad** de la información. Para esta etapa de identificación de amenazas y vulnerabilidades se debe remitir a la lista citada en la guía *"Lineamientos del Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas" versión 2025* emitida por el MinTIC.

Para cada riesgo, se pueden asociar el grupo de activos o activos específicos del proceso, y analizar conjuntamente las posibles amenazas y vulnerabilidades que podrían causar su materialización

b) Análisis del riesgo inherente:

- **Determinar la probabilidad:** se debe realizar el análisis de probabilidad de la materialización de estos riesgos.

Probabilidad	Frecuencia de la Actividad
Muy Baja – 20%	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año
Baja – 40%	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año
Media – 60%	La actividad que conlleva el riesgo se ejecuta de 25 a 500 veces por año
Alta .80%	La actividad que conlleva el riesgo se ejecuta más de 500 veces al año y máximo 5000 veces por año
Muy Alta – 100%	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año

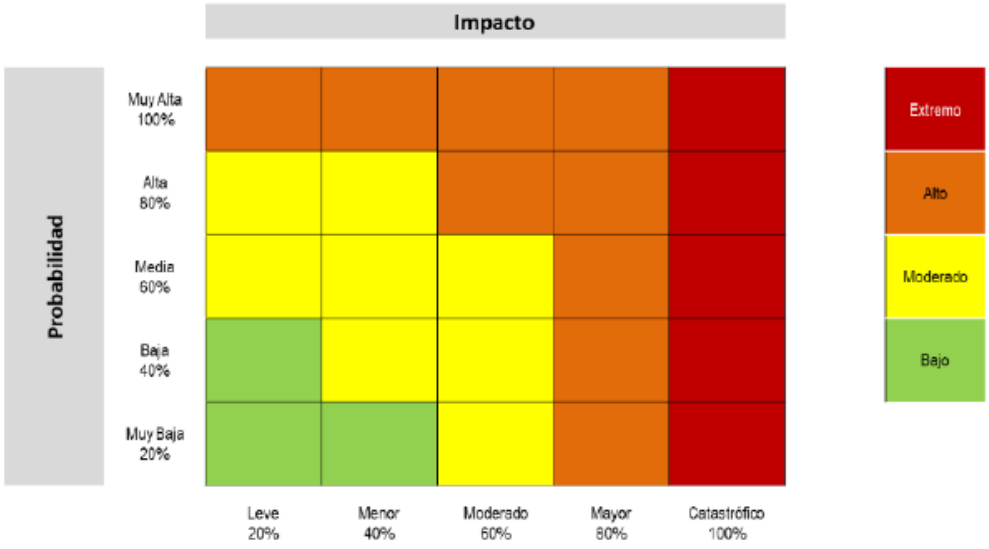
Fuente: Guía para la Gestión Integral del Riesgo en Entidades Públicas Versión 7.

- **Determinar el impacto:** se debe realizar el análisis del impacto de la materialización de estos riesgos.

Nivel de Impacto	Afectación Económica	Afectación Reputacional
Leve-20%	Afectación menor a 10 SMLMV	El riesgo afecta la imagen de algún área de la entidad.
Menor-40%	Mayor a 10 SMLMV y Menor a 50 SMLMV	El riesgo afecta la imagen de la entidad a nivel interno, de conocimiento general, de junta directiva y accionistas y/o de proveedores.
Moderado-60%	Mayor a 50 SMLMV y Menor a 100 SMLMV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos.
Mayor-80%	Mayor a 100 SMLMV y Menor a 500 SMLMV	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal.
Catastrófico-100%	Mayor a 500 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país

Fuente: Guía para la Gestión Integral del Riesgo en Entidades Públicas Versión 7.

- **Análisis de severidad:** se determina la zona de severidad de la matriz de calor en la cual se encuentra el riesgo, según su probabilidad e impacto.



Fuente: Guía para la Gestión Integral del Riesgo en Entidades Públicas Versión 7.

c) Diseño y análisis de controles:

Después de establecidos y valorados los riesgos inherentes se procede a establecer los controles asociados, usando como mínimo los controles del Anexo A de la ISO/IEC 27001:2022, para determinar las cualidades y características de cada control, con el fin de realizar una evaluación a la efectividad para validar que el impacto de riesgo se

logró minimizar alcanzando niveles deseados de aceptación del riesgo. En esta etapa se debe especificar si el control es de tipo preventivo, detectivo o correctivo; el tiempo o periodicidad con que el control se implementará y los responsables de ejecutarlo.

d) Valoración del riesgo residual

El objetivo de esta etapa es identificar las opciones para tratar los riesgos de acuerdo con el nivel de riesgo residual obtenido, esto para procesos en funcionamiento, pero cuando se trate de procesos nuevos se procede a partir del riesgo inherente.
Las estrategias en el tratamiento de riesgos consisten en minimizar la probabilidad de materialización del riesgo. Para ello, se debe identificar y formalizar las opciones de tratamiento adecuadas, dentro de las cuales se encuentran:

- **Evitar**: Después de realizar un análisis y considerar que el nivel del riesgo es demasiado alto, se determina NO asumir la actividad que genera este riesgo.

- **Aceptar**: 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.

- **Reducir:** Después de realizar un análisis y considerar que el nivel de riesgo es alto, se determina tratarlo mediante mitigar o compartir el riesgo.

    - **Compartir**: Cuando es muy difícil para la entidad reducir el riesgo a un nivel aceptable o se carece de conocimientos necesarios para gestionarlo, este puede ser compartido con otra parte interesada que pueda gestionarlo con más eficacia.

    - **Mitigar**: Se adoptan medidas para reducir la probabilidad o el impacto del riesgo, o ambos; mediante el establecimiento de controles para que el riesgo residual se pueda reevaluar como algo aceptable para la Institución.

Una vez se han identificado los riesgos residuales se debe diseñar un plan de tratamiento para los riesgos identificados, en el cual se defina un listado de controles a implementar con el fin de reducir el nivel de riesgo a un estado tolerable o de aceptación por parte de los gestores o dueños de procesos y quiénes serán los responsables de esta implementación. Este plan debe plantear claramente cada acción, etapa y procedimientos que se ejecutarán para poder ser monitoreado y lograr el seguimiento a la ejecución del mismo.

8.2. FASE DE EJECUCIÓN

Esta fase consiste en la ejecución y cumplimiento de los planes de tratamiento diseñados previamente. Para ello, la alta dirección debe garantizar los recursos, mientras que el responsable de seguridad de la información supervisa que la Primera Línea de Defensa cumpla con las tareas, tiempos y presupuestos acordados.

8.3. FASE DE MONITOREO Y REVISIÓN

En esta fase se debe hacer monitoreo de los riesgos y seguimiento a los planes de tratamiento con el fin de evaluar la efectividad de las medidas de control establecidas y su impacto en la disminución de la valoración del riesgo para así determinar su relevancia y actualizarlas si es necesario.

El monitoreo y revisión de los riesgos se realizará en primera instancia, por los responsables del proceso, quiénes son los encargados de realizar las acciones asociadas a los controles establecidos para cada uno de los riesgos identificados para su proceso, de acuerdo con la periodicidad establecida.

En segunda instancia este monitoreo lo deberá realizar la Oficina de Control Interno mediante auditorías internas programadas, con el fin de analizar el diseño e idoneidad de los controles, determinando si son o no adecuados para prevenir o mitigar los riesgos de los procesos y sugerir los correctivos y oportunidades de mejora a los riesgos identificados.

8.4. FASE DE MEJORAMIENTO CONTINUO DE LA GESTION DE RIESGOS DE SEGURIDAD DIGITAL

El Plan de Tratamiento de Riesgos de Seguridad de la Información será revisado y actualizado periódicamente, o ante cambios relevantes en los procesos, sistemas, amenazas o normatividad, incorporando los resultados de auditorías internas y externas para definir acciones correctivas y preventivas que fortalezcan la gestión del riesgo y protejan la confidencialidad, integridad y disponibilidad de los activos de información críticos.

9. 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*

Versión	Fecha	Cambios	Elaboró/Modificó	Revisó	Aprobó
02	27/09/2022	Se reestructuró el documento y sus actividades.	Mónica Hernández *Prof. Seguridad de la Información*	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	06/02/2025	Se actualizó el plan para la vigencia 2025.	Mónica Hernández *Prof. Seguridad de la Información*	*Roiman A. Sastoque Jefe Oficina de Sistemas*	*Roiman A. Sastoque Jefe Oficina de Sistemas*
05	30/01/2026	Se actualizó el plan para la vigencia 2026.	Mónica Hernández *Prof. Seguridad de la Información*	*Roiman A. Sastoque Jefe Oficina de Sistemas*	*Roiman A. Sastoque Jefe Oficina de Sistemas*