INSTITUCIÓN UNIVERSITARIA
MAYOR DE CARTAGENA

AVANZA
HACIA LA EXCELENCIA

# PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN - TRSPI

TABLA DE CONTENIDO

# 1. INTRODUCCIÓN

El **Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información** es un documento estratégico que establece las acciones necesarias para mitigar, aceptar, transferir o evitar los riesgos identificados en los sistemas de información de la institución universitaria. Este plan se diseña en cumplimiento de los lineamientos establecidos por el **Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC)**, enmarcado en las políticas nacionales de seguridad digital, privacidad y protección de datos personales.

La creciente dependencia de la tecnología en los procesos académicos y administrativos de nuestra institución genera desafíos significativos en la gestión de riesgos asociados a la seguridad de la información. Este documento busca garantizar la **confidencialidad, integridad y disponibilidad de los datos** que manejamos, protegiendo tanto los derechos de nuestros usuarios como la continuidad operativa de los servicios institucionales.

Con este esfuerzo, la institución se compromete a robustecer su postura de seguridad y privacidad, alineándose con el marco regulatorio vigente y con las mejores prácticas internacionales, promoviendo una cultura organizacional orientada a la gestión proactiva de riesgos en un entorno digital en constante evolución.

## 2. OBJETIVOS

### 2.1 Objetivo General

Establecer las estrategias y acciones necesarias para tratar los riesgos relacionados con la seguridad y la privacidad de la información en la Institución Universitaria Mayor de Cartagena. Estos riesgos pueden afectar la confidencialidad, integridad y disponibilidad de la información crítica, así como la protección de los datos personales de estudiantes, académicos, personal administrativo y otros involucrados. El plan busca minimizar posibles daños, cumplir con la normativa vigente y garantizar un entorno seguro para el manejo de la información.

## 3. ALCANCE

Este plan abarca todos los sistemas de información, procesos y datos gestionados por la Institución Universitaria Mayor de Cartagena que puedan estar expuestos a riesgos de seguridad y privacidad. Incluye tanto la infraestructura tecnológica (como redes, servidores y equipos) como el comportamiento de los usuarios que acceden a la información. Además, cubre todos los departamentos y unidades administrativas de la universidad, tanto en sus instalaciones físicas como en ambientes virtuales.

## 4. NORMATIVA Y REFERENCIAS

| Normativa/Estándar | Descripción | Ámbito |
|---|---|---|
| **Constitución Política de Colombia** | Garantiza los derechos fundamentales, incluyendo la privacidad y protección de los datos personales. | Derechos fundamentales, privacidad |
| **Ley 1581 de 2012 - Protección de Datos Personales** | Regula el tratamiento y protección de los datos personales en Colombia. | Datos personales, privacidad |
| **Decreto 1377 de 2013** | Reglamenta la Ley 1581 de 2012, proporcionando directrices específicas para la protección de datos personales. | Datos personales, privacidad |
| **Ley 1273 de 2009 - Delitos Informáticos** | Penaliza los delitos que comprometen la seguridad informática, como el acceso no autorizado y el fraude electrónico. | Ciberseguridad, delitos informáticos |
| **Circular Externa 002 de 2015 (SIC)** | Define las medidas mínimas de seguridad para el tratamiento de datos personales, exigiendo controles de acceso y protección de la información. | Datos personales, seguridad de la información |
| **ISO/IEC 27001** | Estándar internacional para implementar un Sistema de Gestión de Seguridad de la Información (SGSI), aplicable en Colombia. | Seguridad de la información |

| Normativa/Estándar | Descripción | Ámbito |
|---|---|---|
| ISO/IEC 27002 | Proporciona controles y mejores prácticas para la seguridad de la información, complementando la ISO/IEC 27001. | Seguridad de la información |
| Guía de Implementación de un SGSI (MinTIC) | Apoya la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en ISO 27001. | Seguridad de la información |
| Política Nacional de Seguridad Digital (MinTIC) | Establece directrices para proteger los activos de información a nivel nacional, con enfoque en ciberseguridad. | Ciberseguridad, seguridad digital |
| CONPES 3854 de 2016 | Política Nacional de Ciberseguridad, orienta acciones para proteger la infraestructura crítica y la información digital en Colombia. | Ciberseguridad, seguridad digital |
| CONPES 3701 de 2011 | Política Nacional de Protección de Datos Personales, regula el tratamiento adecuado de los datos personales y protege los derechos de privacidad. | Datos personales, privacidad |
| Decreto 1078 de 2015 | Incluye regulaciones sobre ciberseguridad y protección de datos en el sector de las Tecnologías de la Información y Comunicaciones (TIC). | Ciberseguridad, seguridad digital |
| Decreto 886 de 2014 | Establece sanciones por incumplimiento de la Ley 1581 de 2012 en cuanto a la protección de datos personales. | Datos personales, sanciones |
| Ley 1915 de 2018 | Modifica el régimen de derecho de autor, incluyendo la protección digital de contenidos y datos relacionados con derechos de autor. | Propiedad intelectual, seguridad digital |
| Decreto 612 de 2018 | Reglamenta el uso de medios electrónicos en el sector público para mejorar la eficiencia administrativa. | Gobierno digital, ciberseguridad |
| Decreto 2106 de 2019 | Simplificación de trámites y procedimientos administrativos, promoviendo el uso de tecnologías de la información. | Administración pública, ciberseguridad |
| Ley 1952 de 2019 - Código General Disciplinario | Establece las normas de conducta y responsabilidad de los funcionarios públicos, incluyendo la protección de datos y transparencia. | Transparencia, seguridad de la información |

## 5. DEFINICIONES Y TÉRMINOS CLAVES

Para facilitar la comprensión de este plan, es importante definir algunos términos clave que se utilizarán:

- **Riesgo de seguridad de la información:** Situación que podría comprometer la confidencialidad, integridad o disponibilidad de la información.
- **Riesgo de privacidad:** Posible amenaza a los datos personales que podría afectar los derechos de las personas involucradas.
- **Activo:** Cualquier recurso valioso para la universidad, como la información, el hardware, el software o las personas.
- **Amenaza:** Cualquier circunstancia o evento que podría dañar los activos o interrumpir su funcionamiento.
- **Vulnerabilidad:** Debilidad en los sistemas o procesos que puede ser explotada por una amenaza.
- **Tratamiento de riesgos:** Estrategias que se implementan para reducir o eliminar los riesgos identificados.
- **Mitigación de Riesgos:** Acciones destinadas a reducir la probabilidad o el impacto de un riesgo sobre la seguridad de la información.
- **Infraestructura Crítica:** Sistemas o activos, físicos o virtuales, esenciales para la operación de una sociedad, cuya interrupción o destrucción tendría un grave impacto en la seguridad pública, la salud o la economía.
- **Seguridad de la Información**: Proceso continuo que incluye la protección de la información de una organización frente a amenazas, garantizando su confidencialidad, integridad y disponibilidad.
- **Política de Seguridad de la Información**: Conjunto de principios, reglas y controles que una organización establece para proteger la información que maneja frente a riesgos o amenazas.
- **Gestión de Riesgos:** Proceso continuo de identificación, evaluación y mitigación de riesgos para minimizar el impacto de amenazas sobre la seguridad de la información.
- **Protección de Datos Personales:** Conjunto de principios, derechos y obligaciones establecidos por la ley para garantizar que los datos personales sean tratados con respeto a la privacidad del titular.
- **Incidente de Seguridad**: Suceso que afecta la confidencialidad, integridad o disponibilidad de la información o de los sistemas de información, incluyendo ciberataques, pérdida de datos o accesos no autorizados.
- **Ciberseguridad**: Conjunto de medidas y controles diseñados para proteger los sistemas informáticos, las redes y los datos contra ataques, daños o acceso no autorizado.

- **Confidencialidad:** El principio según el cual la información solo debe estar disponible y ser accesible por personas autorizadas.
- **Integridad de la Información:** Garantía de que la información no ha sido alterada o modificada de manera no autorizada, asegurando su exactitud y completitud.
- **Disponibilidad de la Información:** Asegurar que la información esté accesible y utilizable cuando sea requerida por una persona autorizada.

- **Datos Personales**: Cualquier información vinculada o que pueda asociarse a una persona natural identificada o identificable, como el nombre, cédula, dirección, correo electrónico, entre otros. Su protección está garantizada por la Ley 1581 de 2012.
- **Datos Sensibles**: Aquellos datos que afectan la intimidad del titular o cuyo uso indebido puede generar discriminación, como los datos sobre origen racial o étnico, orientación política, salud, vida sexual, o datos biométricos.

# 6. CONTEXTO

## 6.1 Contexto Organizacional

La Institución Universitaria Mayor de Cartagena, una institución cuyo principal activo es la información académica, investigativa y administrativa que gestiona. Esta información incluye datos personales de estudiantes, profesores, empleados y terceros, así como datos financieros, investigaciones científicas y documentos estratégicos. Debido a la naturaleza de su actividad, Umayor está expuesta a múltiples riesgos en el ámbito de la seguridad de la información y privacidad de datos personales.

El entorno académico moderno, altamente digitalizado, implica el uso de infraestructuras tecnológicas avanzadas, sistemas de gestión de aprendizaje en línea, plataformas de investigación, servidores de almacenamiento y servicios en la nube. Estos recursos, aunque vitales para el funcionamiento de la universidad, también presentan vulnerabilidades y retos en cuanto a la protección de la información.

*Ver Matriz DOFA institucional.*

## 6.2 Contexto Tecnológico

Umayor cuenta con una infraestructura tecnológica que incluye servidores, redes internas, sistemas de gestión académica, sistemas de información financiera y administrativa, plataformas de educación en línea. Esta infraestructura es fundamental para el funcionamiento diario de la universidad, pero también es susceptible a diversos riesgos tecnológicos, tales como:

- **Ciberataques**: Como phishing, ransomware o accesos no autorizados a través de brechas de seguridad.
- **Fugas de datos:** Por manejo inadecuado de la información, falta de cifrado o errores humanos.
- **Pérdida de integridad de la información:** Por mal funcionamiento de sistemas o fallos en las copias de seguridad.

Dada la creciente dependencia de los sistemas tecnológicos, cualquier interrupción o ataque cibernético puede tener un impacto significativo en la operación diaria, la investigación y los servicios que Umayor presta a la comunidad universitaria.

### 6.3 Partes Interesadas

Existen varias partes interesadas dentro y fuera de la organización que deben ser consideradas en el análisis de riesgos de seguridad y privacidad de la información. Cada parte interesada puede tener diferentes expectativas, responsabilidades y preocupaciones en cuanto a la protección de la información. Algunas de las principales partes interesadas incluyen:

- **Estudiantes:** Son titulares de los datos personales, incluyendo información académica y financiera. Esperan que su privacidad esté garantizada.
- **Docentes e investigadores:** Generan grandes volúmenes de datos, incluidas investigaciones científicas sensibles que deben ser protegidas.
- **Personal administrativo:** responsable de la gestión diaria de la universidad y el manejo de información confidencial.
- **Proveedores de servicios tecnológicos:** Empresas externas que suministran soluciones tecnológicas, como sistemas de gestión de datos y almacenamiento en la nube, quienes deben cumplir con los estándares de seguridad requeridos.
- **Entidades gubernamentales:** Autoridades que regulan y supervisan el cumplimiento de las leyes de protección de datos y ciberseguridad.

*Ver matriz de partes interesadas FT-SM-025*

### 6.4 Análisis del Entorno Externo

Además de las partes interesadas y el contexto interno, Umayor debe considerar factores externos que puedan influir en la gestión de riesgos de seguridad de la información. Estos factores incluyen:

- **Tendencias en ciberseguridad:** La rápida evolución de las técnicas de ataque cibernético, como malware avanzado o explotación de vulnerabilidades en software, requiere una actualización constante de los sistemas de defensa.
- **Regulaciones gubernamentales:** Las políticas de seguridad digital nacionales e internacionales influyen directamente en la forma en que se manejan los datos y se protegen los sistemas.
- **Entorno competitivo:** Otras universidades y centros educativos pueden estar implementando nuevas tecnologías o mejores prácticas de seguridad, lo que presiona a Umayor a mantenerse competitiva y segura.

### 6.5 Análisis de Cultura Organizacional

La cultura organizacional de Umayor también juega un papel importante en la seguridad de la información. Si bien la tecnología es esencial, la formación y concienciación del personal sobre los riesgos de seguridad es igualmente fundamental. Una cultura que promueva buenas prácticas en el manejo de la información, el respeto por las políticas de seguridad y privacidad, y la responsabilidad individual será clave para reducir los riesgos.

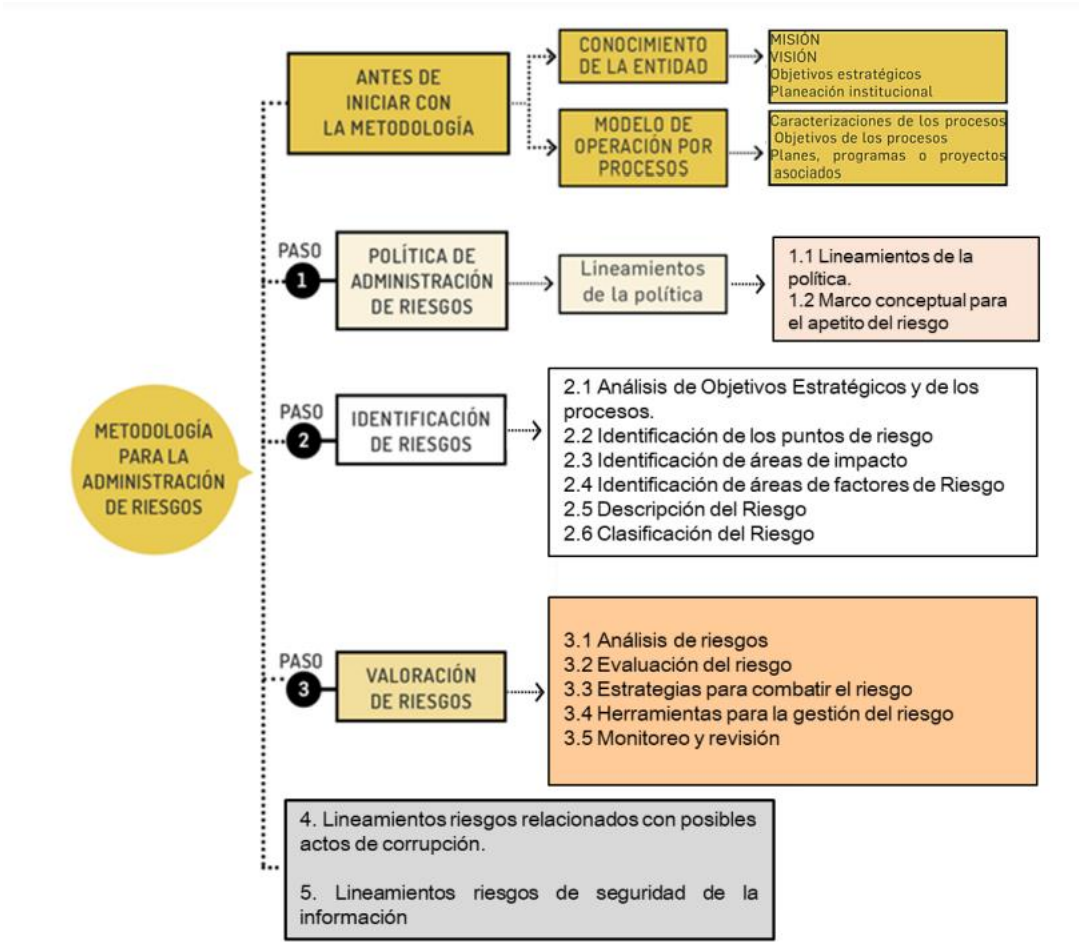
## 7. METODOLOGÍA PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El plan de tratamiento de riesgos de seguridad y privacidad de la información establece una metodología precisa en donde se deriva actividades enfocada a asegurar la protección de la información mediante la identificación de posibles amenazas y vulnerabilidades, la evaluación del impacto que estos riesgos pueden tener sobre la universidad, y la priorización de acciones para mitigar o eliminar los riesgos identificados.

Este proceso garantiza que los riesgos se gestionen de manera eficiente, minimizando el impacto potencial y protegiendo los activos más críticos de la universidad.

El Plan de Tratamiento de Riesgos contempla la definición de las actividades a desarrollar en aras de mitigar los riesgos sobre los activos identificados en la entidad, estas actividades se estructuraron de la siguiente manera, siguiendo las recomendaciones de la Guía para la Administración del Riesgo y el diseño de controles en entidades públicas en su última versión.

*Ilustración 1 Metodología para la administración del riesgo*




*Fuente: Elaborado y actualizado por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.*

## 7.1 Medición

El monitoreo y seguimiento de los riesgos de seguridad y privacidad de la información, así como de los controles y planes de tratamiento asociados, son realizados por el equipo de soporte y desarrollo tecnológico. Este proceso se lleva a cabo conforme a la periodicidad y fechas establecidas en la política de administración de riesgos, verificando los resultados obtenidos y asegurando el registro adecuado de los soportes correspondientes a los controles implementados.

Una vez los procesos reportan el cumplimiento de sus planes de tratamiento y controles, el equipo del área de planeación institucional revisa y valida esta información. El objetivo es consolidar y reportar la gestión del riesgo a través de un indicador diseñado para medir el nivel de implementación de los controles relacionados con los riesgos de seguridad y privacidad de la información.

Dicho indicador permite evaluar el porcentaje de ejecución de los controles definidos, ofreciendo una visión clara del avance en la mitigación de los riesgos identificados en los sistemas de gestión de la entidad, y asegurando una toma de decisiones informada para fortalecer la postura de seguridad de la institución.

## 8. CRONOGRAMA DE IMPLEMENTACION DEL PLAN

Las actividades derivadas en la implementación del plan de tratamiento de riesgo de la seguridad y privacidad de la información son:

| ACTIVIDAD | PRODUCTO | RESPONSABLE | AÑO | FECHA DE CUMPLIMIENTO | | |
|---|---|---|---|---|---|---|
| | | | | I | II | III |
| Realizar inventario y clasificar los activos de información críticos | Inventario de activos críticos de información clasificada por criticidad (CID) | Soporte y desarrollo tecnológico | 2025 | X | | |
| Evaluar los riesgos asociados a los activos de información y priorizar los riesgos identificados. | *Procedimiento y metodología de gestión de riesgos institucional incluyendo el capítulo de seguridad y privacidad de la información aprobado por el comité de coordinación de control interno<br><br>*Matriz de riesgos de seguridad de la información | Soporte y desarrollo tecnológico | 2025 | X | | |
| Implementar controles de seguridad específico para mitigar los riesgos críticos | Evidencias del Plan de tratamiento de riesgos con controles de seguridad asignado a cada activo | Soporte y desarrollo tecnológico | 2025 | | X | X |
| Realizar seguimiento a la implementación de controles de los riesgos asociados a la seguridad y privacidad de la información | Informe con la evaluación y medición de la efectividad de la implementación de los controles definidos en el plan de tratamiento de riesgos. | Soporte y desarrollo tecnológico/Seguimiento y medición | 2025 | | X | X |

Cartagena de Indias - Centro Histórico
K3 # 36-95 Calle de la Factoría
umayorctg

| ACTIVIDAD | PRODUCTO | RESPONSABLE | AÑO | FECHA DE CUMPLIMIENTO | | |
|---|---|---|---|---|---|---|
| | | | | I | II | III |
| Definir y documentar estrategias de continuidad para los activos críticos de Umayor. | Plan de Continuidad de Negocio, incluyendo procedimientos de respaldo y recuperación. (Registrado en el SIG) | Soporte y desarrollo tecnológico | 2025 | X | | |
| Analizar el impacto operativo de la pérdida o alteración de activos críticos. | Reporte de Análisis de Impacto de Negocio y lista de activos priorizados. | Soporte y desarrollo tecnológico | 2025 | | X | |
| Establecer un protocolo de respuesta y recuperación ante incidentes de seguridad. | Plan de Respuesta a Incidentes y registro de pruebas de simulación de incidentes. | Soporte y desarrollo tecnológico | 2025 | | X | |
| Evaluar los riesgos asociados a los activos de información y priorizar los riesgos identificados. | Matriz de riesgos de seguridad de la información | Soporte y desarrollo tecnológico | 2026 | X | | |
| Implementar controles de seguridad específico para mitigar los riesgos críticos | Evidencias del Plan de tratamiento de riesgos con controles de seguridad asignado a cada activo | Soporte y desarrollo tecnológico | 2026 | X | X | X |
| Realizar seguimiento a la implementación de controles de los riesgos asociados a la seguridad y privacidad de la información | Informe con la evaluación y medición de la efectividad de la implementación de los controles definidos en el plan de tratamiento de riesgos. | Soporte y desarrollo tecnológico | 2026 | X | X | X |