PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

2026

1. INTRODUCCIÓN

El plan de tratamiento de riesgos de seguridad de la información de la Universidad, se encuentra alineado con el Plan de Seguridad y Privacidad de la Información, con la GUIA DE ADMINISTRACIÓN DE RIESGOS, que hace parte del Sistema de Gestión institucional, y tiene como fin la definición de actividades técnicas y organizacionales a tener en cuenta e implementar en la entidad, para atender las vulnerabilidades propias de los activos de información institucionales, en procura de reducir la pérdida de confidencialidad, integridad y disponibilidad de estos.

Adicionalmente, permite el fortalecimiento de los procesos y procedimientos que hacen parte de las medidas técnicas adoptadas como parte de la gestión de riesgos

2. OBJETIVOS

GENERAL

Establecer las acciones a desarrollar durante la vigencia 2026, en el marco de la implementación de controles requeridos para mitigar los riesgos de seguridad de la información asociados a los diferentes activos de información institucionales.

ESPECÍFICOS

- Implementar acciones de tipo técnico que permitan gestionar los riesgos de seguridad de la información.
- Implementar acciones de tipo organizacional que permitan gestionar los riesgos de seguridad de la información.

3. ALCANCE

El Plan de Tratamiento de Riesgos comprende el desarrollo de actividades enmarcadas en la declaratoria de aplicabilidad del MSPI. Debe ser de estricto cumplimiento por parte de los funcionarios, contratistas y terceros que presten sus servicios, o tengan algún tipo de relación con la Universidad, por lo cual, todos los procesos de la Universidad, en especial aquellos que impactan directamente la consecución de los objetivos misionales, deben involucrarse activamente en su ejecución.

4. MARCO NORMATIVO

Marco Normativo	Descripción
Ley Estatutaria 1266 de 2008	Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales.
Ley 1273 de 2009	Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos.
Ley 2012 Estatutaria 1581 de	Por la cual se dictan disposiciones generales para la protección de datos personales.
Decreto 2609 de 2012	Por el cual se reglamenta el Título V de la Ley 594 de 2000 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado".
Decreto 1377 de 2013	Por el cual se reglamenta parcialmente la Ley 1581 de 2012.

Ley 1712 de 2014	Por medio de la cual se crea la Ley de Transparencia ydel derecho de acceso a la Información pública nacional y se dictan otras disposiciones
Decreto 2573 de 2014	Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones.
Decreto 103 de 2015	Por el cual se reglamenta parcialmente la Ley 1712 de2014 y se dictan otras disposiciones
Decreto 1078 de 2015	Modificado por el Decreto 1008 de 2018 - Política de Gobierno Digitalque contiene el Modelo de seguridad y Privacidad - MSPI de MINTIC.
CONPES 3854 de 2016	Política de Seguridad Digital del Estado Colombiano
Decreto 1499 de 2017	El cual modificó el Decreto 1083 de 2015 – Modelo Integrado de Planeación y Gestión.
Ley 1928 de 2018	Por medio de la cual se aprueba el "Convenio sobre La Ciberdelincuencia", adoptado el 23 de noviembre de 2001, en Budapest
CONPES 3995 de 2020	Política Nacional De Confianza y Seguridad Digital
Resolución 1519 de 2020	Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos Materia de accesso a la Información publica, accesibilidad web, seguridaddigital, y datos abiertos.
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 500 de 2021.
Resolución 02277 de 2025	Por la cual se actualiza el Anexo 1 de la Resolución 500 de 2021 y se derogan otras disposiciones relacionadas con la materia

- **Modelo de Seguridad y Privacidad de la Información de MINTIC:** Tiene como objetivo preservar la confidencialidad, integridad y disponibilidad de los activos de información, garantizando su buen uso y la privacidad de los datos.

- **NORMA ISO 27001:2022:** Estándar internación que tiene como objetivo sugerir lineamientos y buenas prácticas a cualquier tipo de organización o entidad para el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan.

- **ISO 31000:2018:** Tiene como objetivo sugerir lineamientos y buenas prácticas a cualquier tipo de organización o entidad, para incorporar estándares y procesos de alto nivel para evaluar y mitigar riesgos en todas sus operaciones.

- Guía para la administración del riesgo y el diseño de controles en entidades públicas Riesgos de gestión, corrupción y seguridad digital - Versión 6 emitida por el DAFP.

5. METODOLOGÍA DEL PLAN DE TRATAMIENTO DE RIESGOS

- **Identificación y valoración de activos de información**

Identificación de los responsables de los activos de información quienes son los responsables de realizar la identificación y categorización de estos. La identificación y valoración de activos de información se realiza conforme a lo establecido en el Modelo de Gestión de Riesgos de Seguridad Digital del Anexo 4. Lineamientos para la Gestión de Riesgos de Seguridad Digital en Entidades Públicas, imagen1.

Imagen 1. Pasos para la identificación y valoración de activos.
Fuente: Ministerio de Tecnologías de la Información y Comunicaciones

- **Identificación de riesgos**

Los riesgos asociados a los activos de información institucionales se clasifican en pérdida de la confidencialidad, pérdida de la integridad o pérdida de la disponibilidad.

- **Valoración de amenazas y vulnerabilidades (causas)**

Identificación de amenazas y vulnerabilidades asociadas a los activos de información institucionales según el riesgo valorado, de acuerdo con la Norma ISO 27005 y el Modelo de Gestión de Riesgos de Seguridad Digital del Anexo 4. Lineamientos para la Gestión de Riesgos de Seguridad Digital en Entidades Públicas.

- **Determinación del nivel de riesgo de seguridad de la información**

La determinación del nivel de riesgo de seguridad de la información es la combinación de la valoración de los activos de información, el nivel de amenaza y la valoración de la probabilidad de la vulnerabilidad; para tal fin se definirá la metodología de valoración de riesgos que permita ubicar los riesgos identificados en un mapa de calor de clasificación de riesgos según la criticidad de los activos, de esta ubicación se determina el nivel de riesgo aceptable.

- **Gestión del Riesgo**

De acuerdo con la determinación del Nivel de Riesgo de Seguridad de la Información, se establece para la gestión de riesgos, los siguientes cuatro métodos:

- ACEPTAR EL RIESGO.
- TRATAR EL RIESGO
- TRANSFERIR EL RIESGO
- EVITAR EL RIESGO

6. DESARROLLO DE LA METODOLOGÍA

ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	FECHA
Identificación de riesgos asociados a los activos de información	Identificar aquellos riesgos críticos a los que se encuentran expuestos los activos de información, mediante encuestas realizadas a los procesos o dueños de los activos de información. Luego de identificar los riesgos estos serán registrados en una matriz que permita su clasificación.	Oficial de Seguridad de la Información Líderes de proceso	Junio 2026
Análisis de riesgos de seguridad de la información	Identificar y valorar los riesgos a los cuales están expuestos los activos de información con el fin de establecer controles apropiados de seguridad. En esta fase se definen los criterios que se deben utilizar para evaluar la importancia del riesgo, de acuerdo con el impacto que pueda tener en caso de que este se materialice (Insignificante – Bajo – Moderado – Mayor – Catastrófico).	Oficial de Seguridad de la Información Líderes de proceso	Agosto 2026
Evaluación de los controles establecidos para la mitigación de los riesgos.	Evaluar los controles, luego de haber establecido el riesgo inherente a cada activo de información, el impacto y probabilidad de ocurrencia. La evaluación de controles se realiza identificando los criterios relacionados a cada uno de los riesgos establecidos.	Oficial de Seguridad de la Información Oficina de Tecnologías de la Información y las Comunicaciones	Noviembre 2026
Documentar	Documentar la implementación de controles	Oficial de Seguridad de la Información Oficina de Tecnologías de la Información y las Comunicaciones	Diciembre 2026