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

OFICINA DE SISTEMAS Y TECNOLOGÍA

2025

TABLA DE CONTENIDO

1. OBJETIVOS

1.1. GENERAL

Brindar a la Universidad del Pacífico una herramienta que proporcione las pautas necesarias para el adecuado tratamiento de los riesgos a los que están expuestos los activos de información, de tal forma que se definan y apliquen los controles con los cuales se buscan mitigar la materialización de los mismos, para una adecuada toma de decisiones.

1.2. ESPECÍFICOS

- Consolidar una administración y gestión del riesgo acorde con las necesidades de la institución.
- Proteger los activos de información, de acuerdo a su clasificación y criterios de Confidencialidad, Integridad y Disponibilidad.
- Crear conciencia a nivel institucional de la importancia y la necesidad de una correcta gestión del riesgo de seguridad de la información.
- Cumplir con los requisitos legales, reglamentarios, regulatorios y de las normas técnicas colombianas.

2. ALCANCE

La gestión de riesgos de seguridad de la información y su tratamiento será aplicada sobre cualquier proceso de la Universidad del Pacífico, a través de los principios básicos y metodológicos para la planeación y administración de los riesgos de seguridad de la información; incluye además pautas y recomendaciones para su seguimiento, monitoreo, evaluación y mejora.

3. TERMINOS Y DEFINICIONES

RIESGO: Posibilidad de ocurrencia del evento que tiene un efecto positivo o negativo sobre el producto o servicio generado de un proceso o el cumplimiento de los objetivos institucionales.

RIESGO DE SEGURIDAD DE LA INFORMACIÓN: Posibilidad de que una amenaza concreta que pueda aprovechar una vulnerabilidad para causar una pérdida o daño en un activo de información; estos daños consisten en la afectación de la confidencialidad, integridad o disponibilidad de la información.

RIESGO POSITIVO: Posibilidad de ocurrencia de un evento o situación que n permita optimizar los procesos y/o la gestión institucional, a causa de oportunidades y/o fortalezas que se presentan en beneficio de la entidad.

SEGURIDAD DE LA INFORMACIÓN: Este principio busca crear condiciones de uso confiable en el entorno digital, mediante un enfoque basado en la gestión de riesgos, preservando la confidencialidad, integridad y disponibilidad de la información de las entidades del Estado, y de los servicios que prestan al ciudadano.

AMENAZA: es un ente o escenario interno o externo que puede hacer uso de una vulnerabilidad para generar un perjuicio o impacto negativo en la institución (materializar el riesgo).

VULNERABILIDAD: es una falencia o debilidad que puede estar presente en la tecnología, las personas o en las políticas y procedimientos.

IMPACTO: consecuencias que puede ocasionar a la organización la materialización del riesgo.

PROBABILIDAD: se entiende la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando.

CONTROL O MEDIDA: Medida que permite reducir o mitigar un riesgo.

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

En el marco del Modelo de Seguridad y Privacidad de la Información y el Sistema de Gestión de Seguridad de la Información SGSI, de la Universidad del Pacífico, se busca prevenir los efectos no deseados que se puedan presentar en cuanto a seguridad de la información, por lo cual es importante controlar y establecer los riesgos de seguridad de la información.

El Plan de Tratamiento de Riesgos contempla la definición de las actividades a desarrollar en aras de mitigar los riesgos sobre los activos, estas actividades se estructuraron de la siguiente manera, siguiendo las recomendaciones de la Guía de Gestión de Riesgos de Seguridad y Privacidad de la Información:

GESTIÓN	ACTIVIDADES	RESPONSABLE DE LA TAREA	PROGRAMACIÓN	
			Fecha Inicio	Fecha Final
Gestión de Riesgos	Realizar identificación, valoración y definición del Plan de Tratamiento de Riesgo de Privacidad y Seguridad de la Información	Comité de Calidad	2025/04/01	2025/04/30
	Implementación de controles	Responsables de procesos	2025/04/01	2025/06/30
	Publicación mapas de riesgos	Comité de Calidad	2025/07/15	2025/07/15
	Renovación de herramientas de seguridad adquiridas	Responsables de procesos	2025/04/01	2025/06/30
	Ejecución de pruebas de seguridad tipo análisis de vulnerabilidades	Oficina de Sistemas y Tecnología	2025/10/01	2025/10/15
	Seguimiento fase de tratamiento	Responsables de procesos	2025/08/15	2025/12/30
	Análisis y mejoramiento	Responsables de procesos	2025/08/15	2025/12/30

4.1. RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

A continuación, se visualizan los riesgos de Seguridad de la Información, los cuales se encuentran asociados al Sistema de Gestión de Seguridad de la Información SGSI de la Universidad del Pacífico.

No.	NOMBRE	RESPONSABLE	MONITOREO
1	Afectación de la imagen de la universidad por no destruir de forma segura la información que ya no se utiliza o ha perdido su utilidad	Secretarias dependencias	Directivos
2	Afectación de la información por ataques cibernéticos	Oficina de Sistemas y Tecnología	Responsables de procesos
3	Daño de activos documentales durante la administración, custodia y conservación en el archivo central	Secretarias dependencias	Directivos y jefes de dependencia
4	Desaparición, alteración y/o divulgación no autorizada de información por el uso de contraseñas fáciles de descifrar	Todos los funcionarios	Responsables de procesos
5	Fuga de la información administrada por la Universidad del Pacífico	Todos los funcionarios	Responsables de procesos
6	Hurto o fuga de la documentación ubicada en los archivos de gestión de las dependencias	Secretarias dependencias	Directivos y jefes de dependencia

7	Hurto, pérdida o fuga de información pública reservada o clasificada en la gestión de la plataforma o sistema de gestión de información	Todos los funcionarios	Responsables de procesos
8	Inadecuada información en el sistema de gestión de información debido a que la información no es oportuna, ni veraz, ni completa	Todos los funcionarios	Responsables de procesos
9	Violación de la integridad de la información	Todos los funcionarios	Responsables de procesos

5. MARCO LEGAL

- Constitución Política de Colombia 1991. Artículo 15. Reconoce como Derecho Fundamental el Habeas Data y Artículo 20. Libertad de Información.
- Decreto 612 de 4 de abril de 2018, Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las Entidades del Estado.
- Decreto 1008 de 14 de Junio de 2018, Por el cual se establecen los lineamientos generales de la política de Gobierno Digital.

6. DOCUMENTOS ASOCIADOS

- ✓ L-DE-01 Lineamientos para la Administración del Riesgo.
- ✓ G-EM-01 Guía Para La Formulación, Seguimiento y Evaluación De Planes De Mejoramiento.
- ✓ M-TI-01 Manual de Políticas de Seguridad de la Información.