PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

OFICINA DE SISTEMAS Y TECNOLOGÍA

2025

TABLA DE CONTENIDO

1. OBJETIVOS

1.1. GENERAL

Establecer la estrategia de Seguridad y Privacidad de la Información para la vigencia 2025 de la Universidad del Pacífico, el cual es el de salvaguardar toda la información institucional mediante una gestión de riesgos eficaz y la implementación de controles adecuados. Esta iniciativa se orienta a preservar la confidencialidad, integridad y disponibilidad de los activos de información que respaldan los procesos institucionales, implementando así un entorno seguro y controlado contra posibles amenazas y vulnerabilidades.

1.2. ESPECÍFICOS

- Garantizar que la estrategia de Seguridad de la Información se encuentre alineada con las metas y objetos institucionales.
- Establecer y desarrollar las iniciativas y actividades para el cumplimiento efectivo de la estrategia de Seguridad de la Información.
- Definir las medidas técnicas, administrativas y relacionadas con el desarrollo del personal para la implementación y mejoramiento continuo del Modelo de Seguridad y Privacidad de la Información.
- Planificar el seguimiento, medición y análisis de los controles implementados para la adopción del Modelo de Seguridad y Privacidad de la Información.
- Asegurar el respaldo y compromiso de la dirección a través del apoyo y fortalecimiento de las actividades y acciones encaminadas a la implementación del Modelo de Seguridad y Privacidad de la Información.

2. ALCANCE

Este plan se extiende a todos los procesos, al recurso humano y, en términos generales, a cada activo de información que respalda las diversas operaciones internas de la institución. Es fundamental subrayar que la aplicación efectiva de este plan se alinea directamente con el alcance delineado en la Política de Seguridad de la Información, así como con las pautas establecidas en el Documento Maestro del Modelo de Seguridad y Privacidad de la Información adoptados en la Universidad del Pacífico. Este enfoque estratégico garantiza que las medidas de seguridad implementadas sean coherentes con las directrices más amplias y las mejores prácticas definidas en los marcos normativos y estándares pertinentes.

3. DOCUMENTOS DE REFERENCIA

El Plan Estratégico de Seguridad de la Información se basa en los siguientes documentos, normas y lineamientos para su estructura y funcionamiento:

- Decreto Nacional 767 de 2022, "Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones".
- Resolución 746 de 2022 expedida por el Ministerio de TIC, ""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"
- Guía DAFP Guía para la Administración del Riesgo, "Guía para la Administración del Riesgo y el diseño de controles en entidades públicas"
- Decreto Nacional 612 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", donde se encuentra el presente Plan Estratégico de Seguridad de la Información como uno de los requisitos a desarrollar para cumplir con esta normativa.
- Resolución 500 de 2021 expedida por el Ministerio de TIC, "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".
- CONPES 3995 de 2020, "Política Nacional de Confianza y Seguridad digital"
- Manual de Gobierno Digital – MINTIC
- Modelo de Seguridad y Privacidad de la Información – MINTIC
- Ley Estatutaria 1581 de 2012. Ley de Protección de Datos Personales
- Resolución Rectoral No.060 del 31 de octubre de 2014. Política de Tratamiento y Protección de Datos Personales de la Universidad del Pacífico.

4. ESTADO ACTUAL DE LA ENTIDAD RESPECTO AL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Con el propósito de identificar el nivel de madurez frente a la implementación de los lineamientos y controles establecidos en el Modelo de Seguridad y Privacidad de la Información, la Universidad del Pacífico desarrolló el autodiagnóstico correspondiente a la vigencia 2024 a través del "Instrumento de Identificación de Línea Base de Seguridad de la Información" herramienta proporcionada por el Ministerio de TIC. Este análisis contempla la totalidad de los procesos y activos de información que respaldan las diversas operaciones de la Entidad.

El objetivo fundamental de este autodiagnóstico consiste en evaluar de manera integral la eficacia de las medidas de seguridad existentes y detectar posibles áreas de mejora. Al involucrar todos los procesos y activos de información, garantizamos una evaluación integral que nos permita identificar y abordar de manera proactiva cualquier vulnerabilidad o riesgo potencial sobre los activos de información e infraestructura tecnológica.

4.1. EVALUACIÓN DE EFECTIVIDAD DE CONTROLES

Este componente se encarga de medir el grado de implementación de los diferentes Dominios y sus objetivos de control definidos en el Anexo A de la Norma ISO 27001:2023. Dentro de los resultados obtenidos para este componente se puede evidenciar que la Universidad del Pacífico se encuentra en un nivel de implementación "Repetible" de acuerdo con los parámetros de evaluación establecidos en el Instrumento de Evaluación definido por el Ministerio de las TIC.

Frente al análisis realizado sobre este componente se puede evidenciar que los diferentes controles que se han implementado impactan positivamente los diferentes procesos, pero se requiere de un mejoramiento continuo que permita lograr una formalización, comunicación y adopción adecuada sobre las buenas prácticas establecidas y procedimientos de seguridad de la información en toda la institución.

No.	DOMINIO	Calificación Actual	Calificación Objetivo	Evaluación de Efectividad de Control
A.5	Políticas de Seguridad de la Información	80	100	Gestionado
A.6	Organización de la Seguridad de la Información	32	100	Repetible
A.7	Seguridad de los Recursos Humanos	34	100	Repetible
A.8	Gestión de Activos	20	100	Inicial
A.9	Control de Acceso	38	100	Repetible
A.10	Criptografía	10	100	Inicial
A.11	Seguridad Física y del Entorno	33	100	Repetible
A.12	Seguridad de las Operaciones	29	100	Repetible
A.13	Seguridad de las Comunicaciones	42	100	Efectivo
A.14	Adquisición, Desarrollo y Mantenimiento de Sistemas	40	100	Repetible
A.15	Relaciones con los Proveedores	20	100	Inicial
A.16	Gestión de Incidentes de Seguridad de la Información	20	100	Inicial
A.17	Aspectos de Seguridad de la Información de la Gestión de la Continuidad del Negocio	30	100	Repetible
A.18	Cumplimiento	46	100	Efectivo
PROMEDIO EVALUACIÓN DE CONTROLES		**34**	**100**	**Repetible**

5. ESTRATEGIAS DE SEGURIDAD DIGITAL

La Universidad del Pacífico desarrollará una estrategia integral de seguridad de la información alineada con los estándares y buenas prácticas establecidas en el Modelo de Seguridad y Privacidad de la Información. Esta iniciativa se materializará a través de la implementación de políticas, manuales, procedimientos, formatos y la adopción de mecanismos técnicos, administrativos y relacionados con el talento humano.

El propósito fundamental de esta estrategia es asegurar de manera efectiva la información, la infraestructura tecnológica y todos los activos de información de la Universidad del Pacífico. Se pondrá un énfasis especial en preservar la confidencialidad, integridad y disponibilidad de la información institucional.

Esta estrategia estará fundamentada en un enfoque proactivo de gestión de riesgos de seguridad de la información, acompañado de la implementación de controles efectivos para una mitigación adecuada. Se establecerán, además, estrategias específicas destinadas a la gestión oportuna y adecuada de incidentes de seguridad digital y el establecimiento de una cultura de seguridad de la información, orientada a fortalecer las habilidades de todos los usuarios y terceros dentro de la entidad. Además, se implementarán estrategias específicas orientadas a la protección de la información de los ciudadanos, reafirmando nuestro compromiso de ofrecer servicios confiables y seguros a través de las Tecnologías de la Información y las Comunicaciones.

Esta iniciativa no solo busca cumplir con estándares de seguridad, sino también consolidar un entorno digital que promueva la confianza y la transparencia en todas nuestras operaciones. A través de esta estrategia, la Universidad del Pacífico se compromete a mantenerse a la vanguardia en la protección de la información y asegurando la continuidad de los servicios prestados.

6. DEFINICIÓN DE ACTIVIDADES ASOCIADAS AL PLAN ESTRATEGICO DE SEGURIDAD DE LA INFORMACIÓN

La Universidad del Pacífico define los siguientes proyectos y actividades con el propósito de avanzar en la implementación del Modelo de Seguridad y Privacidad de la Información.

- ✓ Liderazgo de seguridad de la información.
- ✓ Gestión de riesgos.

- ✓ Concientización.
- ✓ Implementación de controles.
- ✓ Gestión de incidencias.

7. CRONOGRAMA DE ACTIVIDADES

Teniendo en cuenta los proyectos y actividades definidos en la sección anterior, se establece el siguiente cronograma con el propósito de definir los tiempos estimados para la realización de las actividades planteadas.

ACTIVIDAD	MESES											
	1	2	3	4	5	6	7	8	9	10	11	12
Seguimiento, monitoreo y actualización a las políticas, manuales, procedimientos, guías, formatos, entre otros asociados a Modelo de Seguridad y Privacidad de la Información												
Diseñar y ejecutar los proyectos que permitan la correcta implementación de las actividades y estrategias de seguridad de la información al interior de la entidad.												
Seguimiento, monitoreo y actualización al mapa de riesgos de seguridad de la información.												
Seguimiento, monitoreo y actualización al inventario de activos de información.												
Diseño de una estrategia que permita hacer seguimiento al Plan de tratamiento de riesgos de seguridad de la información de la entidad.												
Implementar una estrategia de capacitación, sensibilización y concientización en temas relacionados con la seguridad y privacidad de la información, dirigido a funcionarios, contratistas y personal de nivel directivo.												
Diseñar una estrategia que permita a la entidad realizar un análisis externo de cumplimiento de los controles asociados a la norma ISO 27001.												
Realizar un ejercicio interno basado en cumplimiento de los requisitos de la norma ISO 27001.												
Hacer Seguimiento, monitoreo y actualización a los indicadores asociadas al Modelo de Seguridad y Privacidad de la Información.												
Realizar de manera semestral un ejercicio de análisis de vulnerabilidades al interior de la entidad.												
Diseñar y ejecutar el plan de implementación de los controles para la remediación de las vulnerabilidades encontradas.												
Implementar los lineamientos y actividades descritas en el procedimiento y la guía de gestión de incidentes de Seguridad de la Información												
Realizar un ejercicio semestral que permita validar los tiempos de respuesta y acciones descritas en el procedimiento de gestión de incidentes de seguridad digital.												

8. ANÁLISIS PRESUPUESTAL

Con base en los proyectos definidos a continuación se mencionan aquellos ítems relacionados con seguridad de la información del cual se tiene conocimiento que se

recomiendan sean incluidos como mínimo en los proyectos mencionados, de igual forma se recomienda durante el primer semestre de 2025 realizar una revisión de este documento y de ser necesario ajustarlo de acuerdo con las proyecciones de la administración entrante.

PROYECTO	FUENTE FINANCIACION	VALOR
Adquisición y renovación de dispositivos de comunicación para el centro de datos de la Universidad del Pacífico	Estampilla Pro Unipacifico	$280.000.000
Renovación de licencias antivirus	Estampilla Pro Unipacifico	$10.000.000
Adquisición de Firmas digitales y Certificados SSL	Nación	$20.000.000
Implementación de sistema de gestión documental	Estampilla Pro Unipacifico	$200.000.000
Adquisición de equipos servidores para el resguardo y almacenamiento de información digital	Estampilla Pro Unipacifico	$250.000.000
Adquisición y renovación del sistema de seguridad perimetral y circuito cerrado de televisión	Estampilla Pro Unipacifico	$240.000.000

9. RESPONSABLES

- Rectoría
- Oficina Asesora de Planeación
- Dirección Administrativa y Financiera
- Oficina de Sistemas y Tecnología
- Oficina de Mantenimiento de Equipos de Cómputo