Contenido

NOTA

La UPN publica la versión preliminar de este documento que se actualizará para alinearlo a los planes del sector y de la entidad, razón por la cual este documento está sujeto a cambios.

1. INTRODUCCIÓN Y CONTEXTO

La información es uno de los activos más valiosos y primordiales para la UPN y se protege asegurando: la disponibilidad, integridad y confidencialidad, estas características apoyan el cumplimiento de la misionalidad de la universidad. Para lograr una protección adecuada de la información, se hace necesaria la gestión de riesgos que puedan afectar los componentes e infraestructura física y lógica que interviene en el tratamiento de la información. (concepto conocido como activos de información).

La defensa y protección de los activos de información es una tarea esencial para asegurar la continuidad de los servicios tecnológicos y el desarrollo de los objetivos institucionales, así como para mantener el cumplimiento normativo y regulatorio aplicable a la entidad, además brinda confianza a las partes interesadas y a la comunidad universitaria.

El presente documento contiene las actividades planeadas para ejecutar en la vigencia 2025 para la optimización y mejora de las condiciones de seguridad de la información de la UPN, el cual toma como referencia el Modelo de Seguridad y Privacidad de la estrategia de Gobierno Digital[1] , así como los elementos que lo componen y descritas en la Resolución 500 de marzo 10 de 2021[2]. Las anteriores normas y esquemas se complementan con el estándar NTC-ISO/IEC 27001:2022 conocido como "*Sistemas de Gestión de Seguridad de la Información*". Esta norma establece los requisitos para el subsistema de seguridad de la información, así como los controles necesarios para el tratamiento de los riesgos típicos que pueden afectar la información y sus servicios asociados.

2. ALCANCE DEL SUBSISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.

En la Universidad, el subsistema es de carácter transversal ya que se alinea al alcance de la Política de Seguridad de la Información (MNL001GSI) registrado en el ítem 2.3 del documento citado, en el cual se establece lo siguiente: " … *la Política deberá aplicarse por parte de los responsables del manejo de la información, funcionarios, profesores, contratistas y estudiantes) en todas las dependencias e instalaciones de la Universidad Pedagógica Nacional, a sus activos y recursos informáticos en la totalidad de los procesos internos y externos y en las tareas o actividades que desempeñen dentro de la Universidad*".

3. ESTRATEGIA DE SEGURIDAD.

La estrategia de seguridad de la Universidad en la vigencia 2025 se enfoca en continuar el fortalecimiento de las medidas de control, manteniendo un enfoque preventivo que articula los aspectos de tipo técnico y administrativo, así como los asociados al talento humano, para garantizar el mejoramiento continuo del proceso de seguridad.

Los controles de seguridad se materializan por medio de documentos, procesos y actividades, éstas últimas se desarrollan en forma permanente o esporádica, algunas de las cuales se relacionan a continuación:

- Identificación y gestión de riesgos de seguridad de la Información. La entidad cuenta con la herramienta para gestionar el Subsistema de Gestión de Seguridad de la Información (Isolución), en la cual se documentan y gestionan los riesgos de seguridad de la información
- Avance en la creación de una cultura y capacitación en seguridad y prevención de riesgos de la información.
- Realización de actividades de gestión y monitoreo de herramientas que protegen la infraestructura de TI.

[1] https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/portal/Estrategias/MSPI/
[2] https://gobiernodigital.mintic.gov.co/692/articles-162625_recurso_2.pdf

- Incorporación de la seguridad en proyectos de implementación y adopción de tecnologías de la información y ciclo de vida del software.
- Disposición de proceso de autenticación y segregación de funciones y responsabilidades para el uso de servicios y sistemas de información.

4. OBJETIVO DEL PLAN

El objetivo de este plan es avanzar en la implementación del MSPI y propender por la minimización de la probabilidad de ocurrencia de riesgos y el impacto de éstos en caso de su materialización, el avance en la implementación se concreta con la adopción de los requisitos o controles contenidos en el Modelo de Seguridad y Privacidad, en cumplimiento de las disposiciones vigentes.

Para el logro del objetivo antes mencionado, se contemplan los siguientes aspectos los cuales se detallan en actividades a ejecutar en la vigencia, las cuales se detallan en la sección ACTIVIDADES.

- Mantenimiento de la arquitectura de referencia y los componentes de seguridad para la infraestructura tecnológica en la nube y en sitio.
- Seguridad de la información de los usuarios finales mediante el mantenimiento, actualización y apropiación de herramientas y esquemas de seguridad (Ej. Antivirus y OneDrive).
- Mantenimiento y renovación de licenciamiento a los componentes de: procesamiento, almacenamiento, red inalámbrica y plataforma de seguridad perimetral.
- Definición y aplicación del plan de tratamiento de riesgos. Las actividades más relevantes de este frente de trabajo son las siguientes:
    - Realización de campaña de sensibilización, apropiación y prevención de riesgos de seguridad de la información dirigido a estudiantes y personal administrativo.
    - Actualización de parches a nivel de software base para mitigación de vulnerabilidades.
    - Realización de ethical hacking en la plataforma expuesta a Internet.

5. MARCO LEGAL.

Este plan da cumplimento a las normas sobre seguridad y privacidad de la información, algunas de las cuales son las siguientes:

- Decreto 767 de Mayo 16 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 500 de marzo 10 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 (y la resolución 746 del 14 de marzo del 2022 que fortalece algunos aspectos de la Resolución 500).
- Decreto 1078 de 2015: Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- Norma NTC / ISO 27001:2022; Seguridad de la información, ciberseguridad y protección de la privacidad – Sistemas de gestión de seguridad de la información.
- Norma ISO/IEC 27002:2022: Seguridad de la información, ciberseguridad y protección de la privacidad. Controles de seguridad de la información

- Decreto 1008 de 2018: 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
- Norma NTC / ISO 31000:2009: Gestión de Riesgo, Principios y Directrices
- Guía para la Administración Del Riesgo Y El Diseño De Controles En Entidades Públicas versión 6 del Departamento Administrativo de la Función Pública.

6. ACTIVIDADES.

La siguiente tabla detalla las actividades contempladas para la vigencia 2025

Plan de Seguridad y Privacidad de la Información - 2025

Actividad	Fecha/periodo previsto	Descripción / Alcance.
Renovación de licencias de herramientas de seguridad.	Sep 2025 Enero 2026 Marzo 2025 Junio 2025	Incluye las siguientes herramientas: Microsoft 365 (one drive) Firewalls (de red y de aplicación) Antivirus Veeam backup Certificados SSL Firmas digitales
Campaña de concientización y prevención de riesgos.	Trimestre II	Estructuración y ejecución de la campaña con el acompañamiento del Grupo de Comunicaciones dirigido a la comunidad universitaria como mecanismos de prevención de riesgos.
Implementación o actualización de procedimientos de seguridad	Trimestre III	• Implementación del Procedimiento de Gestión de Incidentes de Seguridad. • Actualización del procedimiento de copias de respaldo.
Actualización de la plataforma on premises.	Durante la vigencia	Aplicación de actualizaciones de software (parches) en la plataforma base de la infraestructura on premises de la UPN
Riesgos de seguridad de la información.	(por definir)	Realizar el análisis de riesgos del proceso de Gestión Tecnológica. Liderar el análisis de riesgos de seguridad de la información con las áreas dueñas de procesos.

Actividad	Fecha/periodo previsto	Descripción / Alcance.
Gestión de vulnerabilidades técnicas. (Control 8.8 de la ISO27001:2022)	Vigencia 2025	Obtención, análisis y difusión de vulnerabilidades y alertas de seguridad periódicas remitidas por el ColCERT.

7. CONTROL DE VERSIONES.

Fecha	Versión	Descripción
Marzo 2025	1.0	Creación del plan para la vigencia 2025