PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

INSTITUTO NACIONAL DE FORMACIÓN TÉCNICA PROFESIONAL INFOTEP

2026

Av. Colombia, Barrio Sarie Bay. San Andrés Islas, Colombia / Nit: 892400461-5
Teléfonos: (608) 5121350 - 5126607 / Fax: 5125770 / Email: info@infotepsai.edu.co
https://infotepsai.edu.co @infotepsai
Vigilada MiniEducación

TABLA DE CONTENIDO

1. INTRODUCCIÓN. 3
2. DEFINICIONES/GLOSARIO 4
3. OBJETIVO 6
3.1 OBJETIVOS ESPECÍFICOS 6
4. ALCANCE 7
4.1. Alcance sobre Procesos Institucionales 7
4.2. Alcance sobre Activos de Información 8
4.3. Alcance sobre Partes Interesadas 8
4.4. Alcance Geográfico y Lógico 8
5. DOCUMENTOS DE REFERENCIA 9
5.1. Marco Legal y Normativo Nacional 9
5.2. Marco Técnico y Estándares 10
5.3. Marco Institucional (INFOTEP) 10
6. ESTADO ACTUAL DE LA ENTIDAD RESPECTO AL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN 11
6.1. Análisis de Resultados FURAG (Habilitador de Seguridad) 11
6.2. Brechas Técnicas y Normativas (MSPI vs. Realidad) 11
6.3. Conclusión del Diagnóstico 12
7. ESTRATEGIA DE SEGURIDAD DIGITAL 12
7.1 DESCRIPCIÓN DE LAS ESTRATEGIAS ESPECÍFICAS 13
7.2 PORTAFOLIO DE PROYECTOS / ACTIVIDADES 13
7.3 CRONOGRAMA DE ACTIVIDADES / PROYECTOS 15
8. ANÁLISIS PRESUPUESTAL 18
9. APROBACIÓN 21

Av. Colombia, Barrio Sarie Bay. San Andrés Islas, Colombia / Nit: 892400461-5
Teléfonos: (608) 5121350 - 5126607 / Fax: 5125770 / Email: info@infotepsai.edu.co
https://infotepsai.edu.co @infotepsai

1. INTRODUCCIÓN.

En el actual escenario de transformación digital del Estado colombiano, la información se ha consolidado como el activo estratégico más valioso para las entidades públicas. Para el **Instituto Nacional de Formación Técnica Profesional (INFOTEP)** de San Andrés, Providencia y Santa Catalina, la gestión de este activo trasciende el cumplimiento normativo; constituye un pilar fundamental para garantizar la calidad educativa, la continuidad de la investigación sobre temáticas de insularidad y la preservación de la confianza depositada por la comunidad estudiantil y el sector productivo del archipiélago.

El presente documento constituye el **Plan Estratégico de Seguridad y Privacidad de la Información (PESI)** para la vigencia **2026**, diseñado como la hoja de ruta institucional para transitar de un modelo de seguridad reactivo hacia una postura proactiva, resiliente y gestionada basada en riesgos. Este plan ha sido estructurado en estricto alineamiento con el **Modelo de Seguridad y Privacidad de la Información (MSPI)** definido por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) en el marco de la Política de Gobierno Digital, y adopta las mejores prácticas internacionales establecidas en la norma **NTC-ISO/IEC 27001**.

La implementación de este plan responde a la necesidad imperativa de proteger los activos de información críticos de la institución tales como registros académicos, datos personales de la comunidad educativa, plataformas financieras y propiedad intelectual derivada de la investigación frente a un panorama de amenazas cibernéticas cada vez más sofisticado y complejo. Asimismo, aborda los desafíos operativos derivados de nuestra ubicación geográfica insular, planteando estrategias de redundancia y continuidad operativa que mitiguen los riesgos asociados a la conectividad y la infraestructura física.

A través de la ejecución de este PESI, **INFOTEP** reafirma su compromiso con el cumplimiento de la **Resolución 02277 de 2025**, **Resolución 500 de 2021**, la **Ley**

Av. Colombia, Barrio Sarie Bay. San Andrés Islas, Colombia / Nit: 892400461-5
Teléfonos: (608) 5121350 - 5126607 / Fax: 5125770 / Email: info@infotepsai.edu.co
https://infotepsai.edu.co @infotepsai
Vigilada MiniEducación

1581 de 2012 (Régimen General de Protección de Datos Personales) y la **Ley 1712 de 2014** (Transparencia y Acceso a la Información), integrando la seguridad digital como un habilitador transversal que soporta los procesos misionales de docencia, investigación y proyección social, garantizando en todo momento la **confidencialidad, integridad y disponibilidad** de la información institucional.

2. DEFINICIONES/GLOSARIO

- **Activo de Información**: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas) que tenga valor para la organización y requiera protección.
- **Amenaza**: Causa potencial de un incidente no deseado, que puede dañar un sistema o a la organización. Es una circunstancia desfavorable que puede ocurrir y que, de materializarse, aprovecha una vulnerabilidad.
- **Ciberseguridad**: Capacidad de proteger o defender el uso del ciberespacio de ataques cibernéticos. Se enfoca en la protección de activos de información digitales e infraestructura tecnológica interconectada.
- **Confidencialidad**: Propiedad de la información que garantiza que esta no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.
- **Disponibilidad**: Propiedad de la información de estar accesible y utilizable por solicitud de una entidad autorizada cuando esta lo requiera. Garantiza que los sistemas funcionen cuando se necesitan.
- **Gestión de Incidentes**: Proceso estructurado para detectar, reportar, evaluar, responder y aprender de los eventos que comprometen la seguridad de la información, con el objetivo de restaurar la normalidad operativa lo antes posible.

Av. Colombia, Barrio Sarie Bay. San Andrés Islas, Colombia / Nit: 892400461-5
Teléfonos: (608) 5121350 - 5126607 / Fax: 5125770 / Email: info@infotepsai.edu.co
https://infotepsai.edu.co @infotepsai
Vigilada MiniEducación

- **Integridad**: Propiedad que busca salvaguardar la exactitud y completitud de la información y sus métodos de procesamiento, asegurando que no ha sido modificada de manera no autorizada.
- **IPv6 (Protocolo de Internet versión 6):** Nueva versión del protocolo de internet diseñada para reemplazar a IPv4, proporcionando un número casi ilimitado de direcciones IP y mejoras en la seguridad y eficiencia del tráfico de red.
- **MSPI (Modelo de Seguridad y Privacidad de la Información):** Marco de referencia emitido por MinTIC que establece los lineamientos para la gestión de la seguridad digital en las entidades del Estado, como habilitador de la Política de Gobierno Digital.
- **Oficial de Seguridad Digital (CISO):** Rol de nivel directivo o asesor responsable de establecer y mantener la visión, la estrategia y el programa de seguridad de la información para garantizar que los activos de información estén adecuadamente protegidos.
- **Políticas de Seguridad:** Directrices y orientaciones formales definidas por la Alta Dirección que establecen el marco de actuación y las reglas de negocio para proteger la información y cumplir los objetivos misionales.
- **Riesgo de Seguridad de la Información**: Efecto de la incertidumbre sobre los objetivos de seguridad. Se caracteriza por la combinación de la probabilidad de un evento (amenaza) y sus consecuencias (impacto) negativas sobre la confidencialidad, integridad o disponibilidad.
- **Sistema de Gestión de Seguridad de la Información (SGSI):** Parte del sistema de gestión global de la organización, basada en un enfoque de riesgos, utilizada para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información.
- **Vulnerabilidad**: Debilidad de un activo o control que puede ser explotada por una o más amenazas. Puede estar presente en el software, hardware, procedimientos o en el factor humano.

Av. Colombia, Barrio Sarie Bay. San Andrés Islas, Colombia / Nit: 892400461-5
Teléfonos: (608) 5121350 - 5126607 / Fax: 5125770 / Email: info@infotepsai.edu.co
https://infotepsai.edu.co @infotepsai

- **WAF (Web Application Firewall):** Sistema de seguridad diseñado específicamente para analizar el tráfico HTTP/HTTPS y proteger las aplicaciones web (como portales académicos) contra ataques comunes como inyección SQL, Cross-Site Scripting (XSS) y otros intentos de explotación.

3. OBJETIVO

Fortalecer la integridad, confidencialidad, disponibilidad, autenticidad y no repudio de los activos de información críticos del **Instituto Nacional de Formación Técnica Profesional (INFOTEP)**, mediante el diseño, implementación y operación de una Estrategia de Seguridad Digital alineada con el **Modelo de Seguridad y Privacidad de la Información (MSPI)** del MinTIC.

El propósito central es reducir la exposición al riesgo cibernético a niveles aceptables para la entidad, garantizando la resiliencia de la infraestructura tecnológica que soporta los procesos de formación académica, investigación insular y gestión administrativa, asegurando el cumplimiento de la **Resolución 02277 de 2025, Resolución 500 de 2021** y la **Norma NTC-ISO/IEC 27001:2013** durante la vigencia **2026**.

3.1 OBJETIVOS ESPECÍFICOS

- **Definir la Gobernanza de Seguridad:** Formalizar y mantener actualizado el marco normativo institucional (Políticas, Roles y Responsabilidades), asegurando la alineación estratégica entre la seguridad digital y los objetivos misionales de educación superior y proyección social.
- **Gestionar el Riesgo de Seguridad Digital:** Identificar, valorar y tratar los riesgos de seguridad y privacidad asociados a los activos de información, aplicando una metodología de gestión de riesgos que considere las amenazas emergentes y las particularidades del entorno geográfico insular.

Av. Colombia, Barrio Sarie Bay. San Andrés Islas, Colombia / Nit: 892400461-5
Teléfonos: (608) 5121350 - 5126607 / Fax: 5125770 / Email: info@infotepsai.edu.co
https://infotepsai.edu.co @infotepsai

- **Fortalecer las Capacidades de Defensa:** Implementar controles técnicos y administrativos robustos para la protección de la infraestructura crítica, incluyendo la **transición segura al protocolo IPv6**, el despliegue de seguridad perimetral para aplicaciones web (WAF) y la gestión de vulnerabilidades técnicas.
- **Fomentar la Cultura de Seguridad:** Ejecutar un plan de sensibilización y entrenamiento continúo dirigido a funcionarios, docentes, estudiantes y contratistas, orientado a modificar comportamientos y reducir la superficie de ataque vinculada al factor humano (Ingeniería Social, Phishing).
- **Garantizar la Mejora Continua y el Cumplimiento:** Establecer mecanismos de monitoreo, medición y evaluación del desempeño del SGSI (Auditorías, Indicadores, Revisión por la Dirección), asegurando la efectividad de los controles y la respuesta oportuna ante incidentes de seguridad de la información.

4. ALCANCE

El presente Plan Estratégico de Seguridad y Privacidad de la Información (PESI) tiene una cobertura integral y es de obligatorio cumplimiento para todos los niveles de la estructura organizacional de **INFOTEP**. Su alcance se define bajo las siguientes cuatro dimensiones para garantizar la protección holística de los activos de información:

4.1. Alcance sobre Procesos Institucionales

El plan cubre la totalidad de los procesos caracterizados en el Sistema Integrado de Gestión de la entidad, incluyendo:

- **Procesos Misionales:** Formación Técnica Profesional, Investigación (específicamente proyectos sobre insularidad y desarrollo regional) y Proyección Social.
- **Procesos Estratégicos:** Dirección y Planeación Institucional.

Av. Colombia, Barrio Sarie Bay. San Andrés Islas, Colombia / Nit: 892400461-5
Teléfonos: (608) 5121350 - 5126607 / Fax: 5125770 / Email: info@infotepsai.edu.co
https://infotepsai.edu.co @infotepsai

- **Procesos de Apoyo:** Gestión de Tecnología e Infraestructura, Gestión del Talento Humano, Gestión Financiera, Gestión Jurídica y Gestión Documental.
- **Procesos de Evaluación:** Control Interno y Aseguramiento de la Calidad.

4.2. Alcance sobre Activos de Información

Se incluyen todos los activos de información físicos y digitales que son propiedad de **INFOTEP** o que están bajo su custodia, tales como:

- **Datos Sensibles:** Información personal de estudiantes, historias académicas, datos biométricos y expedientes laborales de funcionarios y docentes.
- **Propiedad Intelectual:** Resultados de investigaciones, contenidos curriculares y desarrollos de software propios.
- **Infraestructura Tecnológica:** Centros de datos, servidores (on-premise y nube), redes de datos (LAN/WLAN), equipos de computación de usuario final y sistemas de información (ERP, LMS, Portales Web).

4.3. Alcance sobre Partes Interesadas

Los lineamientos y proyectos definidos en este PESI aplican a:

- **Servidores Públicos:** Personal administrativo y directivo de planta.
- **Personal Académico:** Docentes de planta, ocasionales y catedráticos.
- **Población Estudiantil:** Estudiantes activos, aprendices y egresados con acceso a servicios institucionales.
- **Terceros:** Contratistas, proveedores de servicios tecnológicos y aliados estratégicos que procesen o almacenen información de la entidad.

4.4. Alcance Geográfico y Lógico

- **Físico:** Sede principal y sedes alternas ubicadas en el Archipiélago de San Andrés, Providencia y Santa Catalina.
- **Lógico:** Entornos de teletrabajo, trabajo remoto y servicios alojados en la nube (SaaS, PaaS, IaaS) gestionados por la institución.

Av. Colombia, Barrio Sarie Bay. San Andrés Islas, Colombia / Nit: 892400461-5
Teléfonos: (608) 5121350 - 5126607 / Fax: 5125770 / Email: info@infotepsai.edu.co
https://infotepsai.edu.co @infotepsai
Vigilada MiniEducación

Este alcance se alinea con lo establecido en la **Política General de Seguridad de la Información** de INFOTEP y da cumplimiento al Artículo 2.2.9.1.1.3 del Decreto 1078 de 2015 respecto a la masificación de la Estrategia de Gobierno Digital.

5. DOCUMENTOS DE REFERENCIA

El diseño, estructura y funcionamiento del presente Plan Estratégico de Seguridad y Privacidad de la Información (PESI) se fundamenta en el marco jurídico colombiano vigente, los estándares internacionales de mejores prácticas y la normatividad interna de **INFOTEP**.

Los documentos rectores que soportan este plan son:

5.1. Marco Legal y Normativo Nacional

- **Decreto 1078 de 2015:** Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones. Específicamente el Título 2, Capítulo 1, referente a las políticas de Gobierno Digital.
- **Decreto 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. Este decreto establece la obligatoriedad del PESI como instrumento de planeación.
- **Resolución 02277 de 2025 y Resolución 500 de 2021 (MinTIC):** Por las cuales se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el Modelo de Seguridad y Privacidad de la Información (MSPI) como habilitador de la política de Gobierno Digital.
- **Ley 1581 de 2012 y Decreto 1377 de 2013:** Régimen General de Protección de Datos Personales, aplicable a la gestión de datos de estudiantes, docentes y administrativos.
- **Ley 1712 de 2014:** Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional.

Av. Colombia, Barrio Sarie Bay. San Andrés Islas, Colombia / Nit: 892400461-5
Teléfonos: (608) 5121350 - 5126607 / Fax: 5125770 / Email: info@infotepsai.edu.co
https://infotepsai.edu.co @infotepsai
Vigilada MiniEducación

- **Ley 1273 de 2009:** Por medio de la cual se modifica el Código Penal y se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos".

5.2. Marco Técnico y Estándares

- **Modelo de Seguridad y Privacidad de la Información (MSPI):** Guías y anexos técnicos vigentes emitidos por el MinTIC.
- **Manual de Gobierno Digital:** Marco de referencia para la habilitación de servicios ciudadanos digitales.
- **Norma Técnica Colombiana NTC-ISO/IEC 27001:2013/2022:** Sistemas de Gestión de la Seguridad de la Información. Requisitos. Estándar base para la definición de controles.
- **Guía de Gestión de Riesgos de Seguridad de la Información:** Metodología recomendada por MinTIC y Función Pública.

5.3. Marco Institucional (INFOTEP)

- **Plan de Seguridad y Privacidad de la Información** (Versiones anteriores y vigente).
- **Política General de Seguridad de la Información de INFOTEP:** Documento maestro que define el compromiso de la Alta Dirección.
- **Manual de Políticas Específicas de Seguridad Digital:** Conjunto de directrices operativas para el control de acceso, gestión de activos y seguridad física.
- **Mapa de Procesos Institucional:** Insumo base para la definición del alcance del SGSI.

Av. Colombia, Barrio Sarie Bay. San Andrés Islas, Colombia / Nit: 892400461-5
Teléfonos: (608) 5121350 - 5126607 / Fax: 5125770 / Email: info@infotepsai.edu.co
https://infotepsai.edu.co @infotepsai
Vigilada MiniEducación

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

Para establecer la línea base estratégica de la vigencia 2025, **INFOTEP** ha realizado un análisis integral que triangula los resultados del autodiagnóstico del MSPI con el desempeño reportado en el **Formulario Único de Reporte de Avance de la Gestión (FURAG)**. Este análisis permite identificar no solo el cumplimiento normativo interno, sino el posicionamiento de la entidad frente a los estándares de la Política de Gobierno Digital.

6.1. Análisis de Resultados FURAG (Habilitador de Seguridad)

De acuerdo con la última medición de desempeño institucional, el Índice de Gobierno Digital para el habilitador de **Seguridad y Privacidad de la Información** ubicó a la entidad en un puntaje de **93.1**, lo cual corresponde a un nivel de madurez **"DEFINIDO"**.

El desglose de los resultados de FURAG evidencia el siguiente estado por componentes:

- **Fortalezas (Puntajes Altos):** La entidad demuestra un cumplimiento destacado en la formalización de políticas y la estructura de gobernanza (existencia de roles y comités), lo que valida el esfuerzo administrativo realizado en vigencias anteriores.
- **Oportunidades de Mejora (Brechas de Puntaje):** Los resultados indican una disminución en el desempeño en los componentes de **"Implementación Técnica"** y **"Gestión de Riesgos"**. Específicamente, FURAG penaliza la falta de evidencia en la adopción del protocolo IPv6 y la ausencia de mediciones de efectividad de los controles, lo cual impacta directamente el índice general.

6.2. Brechas Técnicas y Normativas (MSPI vs. Realidad)

Al contrastar los resultados de FURAG con la revisión técnica interna, se confirman las siguientes brechas críticas que este PESI busca cerrar:

1. **Transición a IPv6 (Requisito Crítico FURAG):** La infraestructura de red actual opera mayoritariamente sobre IPv4. La falta de adopción de IPv6 es

Av. Colombia, Barrio Sarie Bay. San Andrés Islas, Colombia / Nit: 892400461-5
Teléfonos: (608) 5121350 - 5126607 / Fax: 5125770 / Email: info@infotepsai.edu.co
https://infotepsai.edu.co @infotepsai

uno de los factores que más afecta el puntaje en el reporte de Gobierno Digital. Se requiere ejecutar el plan de transición para cumplir con la Resolución 2710 de 2017.

2. **Gestión de Riesgos Dinámica:** Si bien existe una matriz de riesgos, el autodiagnóstico revela que esta no se ha actualizado con la frecuencia necesaria para responder a amenazas emergentes (Ransomware, IA). El FURAG exige que la gestión de riesgos sea un proceso vivo y no solo un documento estático.
3. **Controles de Seguridad Perimetral:** Se identifica la necesidad de fortalecer la defensa en profundidad. La implementación de un **WAF (Web Application Firewall)** es prioritaria para proteger los portales académicos expuestos a internet, un control técnico exigido para elevar el nivel de madurez hacia "Administrado".

6.3. Conclusión del Diagnóstico

La entidad cuenta con una base documental sólida (Políticas), pero enfrenta un estancamiento en la implementación de controles técnicos avanzados.

Conclusión Estratégica: Para mejorar el índice de desempeño en el próximo reporte FURAG y garantizar la seguridad institucional, la estrategia 2026 debe volcarse hacia la **ejecución técnica**: pasar del documento a la configuración de equipos (IPv6, WAF, IPS) y a la apropiación cultural de la seguridad.

7. ESTRATEGIA DE SEGURIDAD DIGITAL

INFOTEP establece su estrategia de seguridad digital integrando los principios, políticas, procedimientos y guías necesarios para la gestión integral de la seguridad y privacidad de la información. Esta estrategia gira en torno a la implementación efectiva del **Modelo de Seguridad y Privacidad de la Información (MSPI)** y se articula con la **Resolución 02277 de 2025 y Resolución 500 de 2021**, asegurando que la seguridad actúe como un habilitador de la transformación digital institucional.

Para la vigencia 2026, la estrategia se desplegará a través de **5 Ejes Estratégicos** (Estrategias Específicas), diseñados para cerrar las brechas identificadas en el diagnóstico FURAG y fortalecer la postura defensiva de la entidad.

Av. Colombia, Barrio Sarie Bay. San Andrés Islas, Colombia / Nit: 892400461-5
Teléfonos: (608) 5121350 - 5126607 / Fax: 5125770 / Email: info@infotepsai.edu.co
https://infotepsai.edu.co @infotepsai

7.1 DESCRIPCIÓN DE LAS ESTRATEGIAS ESPECÍFICAS

A continuación, se describe el objetivo técnico de cada eje estratégico, alineando las actividades operativas con los dominios de control de la norma NTC-ISO/IEC 27001:

ESTRATEGIA / EJE	DESCRIPCIÓN / OBJETIVO ESTRATÉGICO
1. Liderazgo de seguridad y privacidad de la información	Asegurar la gobernanza del MSPI mediante el compromiso visible de la Alta Dirección. Este eje busca formalizar la estructura de roles (CISO), garantizar la asignación presupuestal y aprobar el marco normativo (Políticas v.2026) que regirá la protección de los activos de información.
2. Gestión de Riesgos	Determinar, analizar y valorar los riesgos de seguridad digital y privacidad que amenazan la misión de **INFOTEP**. El objetivo es actualizar la matriz de riesgos institucional para incluir nuevas amenazas (Ransomware, Fuga de Datos) y definir un **Plan de Tratamiento de Riesgos** efectivo que reduzca la exposición a niveles aceptables.
3. Concientización y Cultura	Fortalecer el "Factor Humano" como primera línea de defensa. Este eje implementará un **Plan de Apropiación y Cultura** dirigido a funcionarios, docentes y estudiantes, enfocado en modificar comportamientos inseguros frente a técnicas de ingeniería social, phishing y manejo de datos personales.
4. Implementación de Controles (Hardening)	Planificar y desplegar soluciones tecnológicas y administrativas para blindar la infraestructura crítica. Para 2026, este eje prioriza el **cumplimiento técnico regulatorio** (Transición a IPv6) y la **seguridad perimetral** (WAF) para proteger los servicios académicos expuestos a internet.
5. Gestión de Incidentes	Garantizar la resiliencia institucional mediante la formalización de una capacidad de respuesta organizada ante ciberataques. Se busca estandarizar el ciclo de vida del incidente (Detección, Contención, Erradicación y Recuperación) para minimizar el impacto en la continuidad del servicio educativo.

7.2 PORTAFOLIO DE PROYECTOS / ACTIVIDADES

Para materializar las estrategias descritas, **INFOTEP** define el siguiente portafolio de proyectos para la vigencia 2026. Estos proyectos responden directamente a las debilidades halladas en el autodiagnóstico y a los requisitos de mejora del índice de Gobierno Digital.

Av. Colombia, Barrio Sarie Bay. San Andrés Islas, Colombia / Nit: 892400461-5
Teléfonos: (608) 5121350 - 5126607 / Fax: 5125770 / Email: info@infotepsai.edu.co
https://infotepsai.edu.co @infotepsai

ESTRATEGIA / EJE	PROYECTO / ACTIVIDAD CLAVE	PRODUCTOS O ENTREGABLES ESPERADOS
Liderazgo	**P1. Actualización del Marco Normativo de Seguridad** Revisión integral y actualización de la Política General y los Manuales de Procedimientos para alinearlos a las nuevas realidades tecnológicas.	1. Política de Seguridad y Privacidad (Actualizada y Aprobada). 2. Manual de Roles y Responsabilidades formalizado. 3. Actas de Comité de gestión.
Gestión de Riesgos	**P2. Gestión de Activos y Riesgos 2026** Actualización del inventario de activos críticos y reevaluación de la matriz de riesgos institucional.	1. Inventario de Activos de Información (Valorado y Clasificado). 2. Matriz de Riesgos de Seguridad Digital actualizada. 3. Plan de Tratamiento de Riesgos implementado.
Concientización	**P3. Programa "Cultura Digital Segura INFOTEP"** Ejecución de campañas de sensibilización y talleres prácticos para la comunidad educativa.	1. Cronograma de capacitaciones ejecutado. 2. Material de divulgación (boletines, piezas gráficas). 3. Reporte de evaluación de adherencia a la cultura.
Implementación de Controles	**P4. Fortalecimiento de Infraestructura y Red (Hardening)** Ejecución de controles técnicos avanzados para cumplimiento normativo y protección de aplicaciones web.	1. Diagnóstico y Plan de Transición IPv4 a IPv6 ejecutado. 2. Solución WAF (Web Application Firewall) implementada y configurada. 3. Solución IPS (Intrusion Prevention System) desplegada.

Av. Colombia, Barrio Sarie Bay. San Andrés Islas, Colombia / Nit: 892400461-5
Teléfonos: (608) 5121350 - 5126607 / Fax: 5125770 / Email: info@infotepsai.edu.co
https://infotepsai.edu.co @infotepsai

ESTRATEGIA / EJE	PROYECTO / ACTIVIDAD CLAVE	PRODUCTOS O ENTREGABLES ESPERADOS
Gestión de Incidentes	**P5. Capacidad de Respuesta y Continuidad** Formalización de procedimientos para la atención de incidentes y aseguramiento de la continuidad operativa.	1. Procedimiento de Gestión de Incidentes formalizado y socializado. 2. Informe de pruebas de vulnerabilidades (Ethical Hacking). 3. Plan de Continuidad del Negocio (BCP) actualizado.

7.3 CRONOGRAMA DE ACTIVIDADES / PROYECTOS

El Responsable de Seguridad de la Información (CISO), con base en los proyectos definidos en la sección anterior, establece el siguiente cronograma de ejecución para la vigencia 2026. Este cronograma evidencia cómo se llevarán a cabo los proyectos de manera secuencial y paralela, asegurando el cumplimiento de las fases del ciclo PHVA (Planear, Hacer, Verificar, Actuar).

Vigencia: 2026

PERIODO	EJE / FASE	ACTIVIDAD / PROYECTO	RESPONSABLE	FECHA LÍMITE / DURACIÓN
TRIMESTRE 1 *(Ene - Mar)*	**Diagnóstico**	**1. Autodiagnóstico MSPI:** Valoración del estado actual de la seguridad utilizando el instrumento oficial de MinTIC y revisión documental.	Líder TI / CISO	20/02/2025
	Diagnóstico	**2. Análisis de Vulnerabilidades:** Ejecución de escaneos técnicos para identificar brechas en	Especialista Seguridad	20/02/2025

Av. Colombia, Barrio Sarie Bay. San Andrés Islas, Colombia / Nit: 892400461-5
Teléfonos: (608) 5121350 - 5126607 / Fax: 5125770 / Email: info@infotepsai.edu.co
https://infotepsai.edu.co @infotepsai

PERIODO	EJE / FASE	ACTIVIDAD / PROYECTO	RESPONSABLE	FECHA LÍMITE / DURACIÓN
		la infraestructura tecnológica.		
	Planeación	**3. Actualización Normativa:** Revisión y actualización de la Política General, Manuales Específicos, Roles y Responsabilidades.	Líder TI / CISO	20/03/2025
TRIMESTRE 2 *(Abr - Jun)*	**Planeación**	**4. Gestión de Activos:** Actualización del inventario, clasificación y valoración de activos de información.	Líder TI / CISO	20/04/2025
	Planeación	**5. Gestión de Riesgos:** Actualización de la matriz de riesgos y definición del plan de tratamiento.	Líder TI / CISO	20/05/2025
	Cultura	**6. Plan de Sensibilización:** Diseño y aprobación del plan de capacitación y comunicación en seguridad.	Líder TI / CISO /Comunicaciones	20/05/2025
	Controles	**7. Diagnóstico IPv6:** Elaboración del plan técnico de diagnóstico para la transición del protocolo IPv4 a IPv6.	Líder TI	20/06/2025

Av. Colombia, Barrio Sarie Bay. San Andrés Islas, Colombia / Nit: 892400461-5
Teléfonos: (608) 5121350 - 5126607 / Fax: 5125770 / Email: info@infotepsai.edu.co
https://infotepsai.edu.co @infotepsai

PERIODO	EJE / FASE	ACTIVIDAD / PROYECTO	RESPONSABLE	FECHA LÍMITE / DURACIÓN
TRIMESTRE 3 *(Jul - Sep)*	**Implementación**	**8. Despliegue de Controles:** Ejecución del plan de tratamiento de riesgos (Implementación de WAF, Controles de Acceso).	CISO	20/07/2025
	Controles	**9. Ejecución IPv6:** Ejecución técnica del plan de transición y coexistencia de protocolos IPv4/IPv6.	Líder TI	20/08/2025
	Medición	**10. Indicadores de Gestión:** Establecimiento y primera medición de los indicadores de eficacia del SGSI.	Líder TI / Planeación	20/08/2025
	Evaluación	**11. Auditorías Internas:** Ejecución del plan de revisión y auditoría de cumplimiento del MSPI.	Control Interno	20/09/2025
TRIMESTRE 4 *(Oct - Dic)*	**Mejora**	**12. Planes de Mejoramiento:** Diseño del plan de mejora continua basado en los hallazgos de auditoría y evaluación de desempeño.	Líder TI / CISO	20/11/2025
	Cierre	**13. Revisión por la Dirección:** Presentación de resultados finales a la	Rectoría / CISO	Diciembre 2025

Av. Colombia, Barrio Sarie Bay. San Andrés Islas, Colombia / Nit: 892400461-5
Teléfonos: (608) 5121350 - 5126607 / Fax: 5125770 / Email: info@infotepsai.edu.co
https://infotepsai.edu.co @infotepsai

PERIODO	EJE / FASE	ACTIVIDAD / PROYECTO	RESPONSABLE	FECHA LÍMITE / DURACIÓN
		Alta Dirección y cierre de vigencia.		

Nota: Al finalizar la vigencia, **INFOTEP** realizará una actualización del cronograma, incorporando el estado del avance de los proyectos formulados y ajustando las fechas para la siguiente vigencia si se presentan desviaciones, conforme a lo establecido en la Guía de MinTIC.

8. ANÁLISIS PRESUPUESTAL

Con base en los proyectos definidos en el cronograma de actividades y las necesidades críticas de hardware y software de seguridad identificadas, se presenta la estimación presupuestal para la vigencia 2026.

Este presupuesto incluye la incorporación de un profesional especializado dedicado a la seguridad, la renovación tecnológica del perímetro (Firewall) y la protección de los puntos finales (Antivirus) para funcionarios y docentes.

PROYECTO / ACTIVIDAD ESTRATÉGICA	DETALLE DE LA INVERSIÓN (RUBROS)	PRESUPUESTO ESTIMADO VIGENCIA 2026 (COP)	PROYECCIÓN SOSTENIMIENTO 2027 (COP)
P1. Fortalecimiento del Talento Humano (Gobernanza)	•Contratación de servicios profesionales de un **Ingeniero Especialista en Seguridad de la Información** (dedicación exclusiva) para ejercer como Oficial de Seguridad Digital (CISO), liderar la	**$70.000.000**	75.000.000

Av. Colombia, Barrio Sarie Bay. San Andrés Islas, Colombia / Nit: 892400461-5
Teléfonos: (608) 5121350 - 5126607 / Fax: 5125770 / Email: info@infotepsai.edu.co
https://infotepsai.edu.co @infotepsai

PROYECTO / ACTIVIDAD ESTRATÉGICA	DETALLE DE LA INVERSIÓN (RUBROS)	PRESUPUESTO ESTIMADO VIGENCIA 2026 (COP)	PROYECCIÓN SOSTENIMIENTO 2027 (COP)
	implementación del MSPI y ejecutar la gestión de riesgos.		
P4. Fortalecimiento de Infraestructura y Red	•Adquisición de **Appliance de Firewall de Nueva Generación (NGFW)** con suscripción de servicios de seguridad (IPS, Filtrado Web, VPN) por 1 año. •Adquisición y licenciamiento de solución **WAF (Web Application Firewall)** para protección del portal académico. • Servicios especializados para diagnóstico e implementación del protocolo **IPv6**.	**$ 25.000.000**	$10.000.000 (Renovación Licencias)
P4.1. Protección de Puntos Finales (Endpoint Security)	•Renovación de **150 licencias de FortiClient EDR Antivirus Corporativo / EDR** (Endpoint Detection and Response) para equipos administrativos y docentes, con consola de gestión centralizada en nube.	$ 30.000.000	$32.000.000 (Renovación anual)
P2. Gestión de Riesgos y Ciberseguridad	• Adquisición de **Sistema de Análisis de Vulnerabilidades** automatizado. • Contratación de servicio de **Ethical Hacking** (Pruebas de Pentesting	$ 15.000.000	$ 15.000.000

Av. Colombia, Barrio Sarie Bay. San Andrés Islas, Colombia / Nit: 892400461-5
Teléfonos: (608) 5121350 - 5126607 / Fax: 5125770 / Email: info@infotepsai.edu.co
https://infotepsai.edu.co @infotepsai

PROYECTO / ACTIVIDAD ESTRATÉGICA	DETALLE DE LA INVERSIÓN (RUBROS)	PRESUPUESTO ESTIMADO VIGENCIA 2026 (COP)	PROYECCIÓN SOSTENIMIENTO 2027 (COP)
	caja negra/gris) para auditoría externa de seguridad.		
P3. Cultura Digital Segura	• Desarrollo de material pedagógico y campañas de sensibilización. • Plataforma de *Phishing Simulation* o contratación de talleres especializados.	$ 3.000.000**	$ 3.000.000
P1 y P5. Consultoría y Auditoría (Gobernanza)	• Auditoría interna de cumplimiento ISO 27001 / MSPI. • Apoyo consultivo para la actualización de BCP/DRP.	$ 20.000.000	$ 20.000.000
TOTAL PRESUPUESTO ESTIMADO		$ 163.000.000	**$ 155.000.000**

Nota Aclaratoria:

1. **Firewall:** Se estima un equipo de gama media-alta capaz de soportar el tráfico de la sede principal y las conexiones VPN.
2. **Antivirus:** Se calcula un valor promedio de mercado para soluciones EDR (Endpoint Detection and Response) que ofrecen mayor protección que un antivirus tradicional, cubriendo 150 equipos.

Av. Colombia, Barrio Sarie Bay. San Andrés Islas, Colombia / Nit: 892400461-5
Teléfonos: (608) 5121350 - 5126607 / Fax: 5125770 / Email: info@infotepsai.edu.co
https://infotepsai.edu.co @infotepsai

3. Los valores son aproximados y deben ser validados mediante los respectivos estudios de mercado previos a la contratación, conforme al Manual de Contratación de **INFOTEP**.

9. APROBACIÓN

El presente **Plan Estratégico de Seguridad y Privacidad de la Información (PESI)** para la vigencia **2026** ha sido sometido a revisión, consideración y aprobación por parte de las instancias de gobierno de **INFOTEP**.

Su contenido ha sido validado técnicamente para asegurar la alineación con el Modelo de Seguridad y Privacidad de la Información (MSPI) y estratégicamente para garantizar el cumplimiento de los objetivos misionales de la institución. La aprobación de este documento implica el compromiso de asignación de los recursos financieros, técnicos y humanos descritos en el análisis presupuestal para su ejecución.

Este documento entra en vigencia a partir de la fecha de su firma y su aprobación queda registrada en el **Acta de Comité No. XXXXX** de la fecha correspondiente.

REGISTRO DE APROBACIÓN		
ELABORÓ	**REVISÓ**	**APROBÓ**
Nombre: Jonathan Marín Medicis	**Nombre:** Comité de Gestión y Desempeño	**Nombre:** (Rector/a) Chales Gallardo Humphries
Cargo: Contratista - Oficial de Seguridad Digital	**Cargo:** presidente del Comité	**Cargo:** Rector - Alta Dirección
Fecha: 05-11-2025	**Fecha:** 05-11-2025	**Fecha:** 05-11-2025

Av. Colombia, Barrio Sarie Bay. San Andrés Islas, Colombia / Nit: 892400461-5
Teléfonos: (608) 5121350 - 5126607 / Fax: 5125770 / Email: info@infotepsai.edu.co
https://infotepsai.edu.co @infotepsai

CONTROL DE CAMBIOS		
VERSIÓN	**FECHA VIGENCIA**	**NATURALEZA DEL CAMBIO**
01	5/11/2025	Construcción del PESI alineado a la Resolución 02277 de 2025, ISO 27001 y resultados FURAG.

Av. Colombia, Barrio Sarie Bay. San Andrés Islas, Colombia / Nit: 892400461-5
Teléfonos: (608) 5121350 - 5126607 / Fax: 5125770 / Email: info@infotepsai.edu.co
https://infotepsai.edu.co @infotepsai