PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN ICANH

2025

CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE ILUSTRACIONES

INTRODUCCIÓN

El Plan Estratégico de Seguridad y Privacidad de la Información del Instituto Colombiano de Antropología e Historia (ICANH) se desarrolla con base en los documentos clave sobre seguridad y privacidad de la información, la Política de Gobierno Digital y las mejores prácticas tanto nacionales como internacionales. Su propósito principal es establecer un modelo de seguridad robusto y eficaz que contemple diagnósticos, planificación, implementación y una mejora continua. Este modelo establece políticas y procedimientos alineados con la estrategia institucional del ICANH y está fundamentado en la identificación y gestión de riesgos, con un seguimiento constante para garantizar la efectividad de los controles adoptados.

Además, el plan fomenta la adopción de metodologías que permitan valorar los activos de información y evaluar los riesgos asociados, con el objetivo de reducir al mínimo los impactos negativos. La finalidad es desarrollar un sistema de gestión de seguridad de la información que cumpla con los más altos estándares nacionales e internacionales, protegiendo de manera integral la confidencialidad, integridad y disponibilidad de la información. Asimismo, se busca garantizar el cumplimiento normativo, mitigar riesgos y asegurar la continuidad operativa del ICANH.

1. OBJETIVO

Implementar el Plan Estratégico de Seguridad de la Información (PESI) liderado por el Área Funcional de Tecnologías y Sistemas de Información garantizando la confidencialidad, integridad y disponibilidad de los activos de información del ICANH para la vigencia 2025.

1.1 OBJETIVOS ESPECÍFICOS

- Implementar y comunicar la estrategia de seguridad de la información del ICANH.
- Proteger los activos de información del ICANH.
- Priorizar los proyectos a implementar para la correcta implementación del Sistema de Gestión de Seguridad de la Información (SGSI).
- Asegurar el cumplimiento de las normativas nacionales e internacionales en materia de seguridad digital
- Planificar la evaluación y seguimiento de los controles y lineamientos implementados en el marco del SGSI.
- Incrementar el nivel de madurez en la gestión de la seguridad de la información del ICANH.

2. ALCANCE

Este documento presenta el Plan Estratégico de Seguridad de la información (PESI), detallando el plan de implementación de proyectos, acciones y servicios para el año 2025, orientados a la implementación del Sistema de Gestión de Seguridad de la Información del ICANH para todos sus procesos y servicios en el marco de la NTC/ISO 27001 de 2013.

3. DEFINICIONES

- ***Activo de Información:*** Elementos que contienen información, ya sea pública o no, que una organización posee, genera o controla. Esto incluye datos e información crítica.

- ***Confidencialidad:*** El principio de proteger la información para que solo las personas o entidades autorizadas puedan acceder a ella.

- ***Control:*** Acciones, políticas, procedimientos y prácticas implementadas para gestionar y mitigar los riesgos de seguridad de la información.

- ***Declaración de aplicabilidad:*** Documento que se incluye en el Sistema de Gestión de Seguridad de la Información (SGSI), que detalla qué controles de seguridad se aplican y por qué algunos no se aplican.

- ***Disponibilidad:*** Asegurarse de que la información esté accesible y utilizable por las personas o entidades autorizadas cuando lo necesiten.

- ***Gestión de incidentes de seguridad de la información:*** Proceso mediante el cual una organización identifica, evalúa, responde y aprende de los incidentes que afectan a la seguridad de la información.

- ***Integridad:*** Asegurar que la información no se altere de forma no autorizada y que se mantenga precisa y completa.

- ***ISO/IEC 27001:*** Norma que establece los requisitos para un sistema de gestión de la seguridad de la información (SGSI).

- ***Modelo de Seguridad y Privacidad de la Información:*** Conjunto de políticas, estructuras, procesos y recursos que una organización utiliza para proteger la seguridad y privacidad de la información.

- ***Riesgo:*** La posibilidad de que una amenaza explote una vulnerabilidad en un activo de información, resultando en pérdidas o daños. El riesgo se mide considerando la probabilidad del evento y las consecuencias.

- ***Seguridad de la información:*** La protección de la información mediante la preservación de su confidencialidad, integridad y disponibilidad, asegurando que no esté accesible, alterada o destruida sin autorización.

- ***Sistema de Gestión de Seguridad de la Información (SGSI):*** Un sistema que ayuda a la organización a implementar, mantener y mejorar sus políticas de seguridad de la información, incluyendo la gestión de riesgos y la asignación de recursos.

- ***Vulnerabilidad:*** Debilidad en un activo o control que puede ser explotada por una amenaza para generar un incidente de seguridad. Las vulnerabilidades pueden estar en sistemas, procesos o prácticas mal implementadas.

4. MARCO LEGAL

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

- Implementación de la Política de Gobierno Digital Decreto 1008 de 2018 (Compilado en el Decreto 1078 de 2015, capítulo 1, título 9, parte 2, libro 2-)

- 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”, donde se encuentra el presente Plan Estratégico de Seguridad de la Información (PESI) como uno de los requisitos a desarrollar para cumplir con esta normativa.

- Resolución 500 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”.

- Decreto 767 de 2022 - Política de Gobierno Digital, con el objetivo de transformar digitalmente la gestión pública y optimizar los servicios que el Estado ofrece a la ciudadanía, promoviendo una mayor transparencia, eficiencia y participación.

- Modelo de Seguridad y Privacidad de la Información – MINTIC 2022.

- Plan Estratégico de Tecnologías de Información institucional (PETI) ICANH 2023.

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

El Plan Estratégico de Seguridad de la Información (PESI) y el Sistema de Gestión de Seguridad de la Información (SGSI) están alineados con el Plan Estratégico Institucional, contribuyendo a su cumplimiento. El Modelo de Seguridad y Privacidad de la Información, dentro de la Estrategia de Gobierno Digital, sigue un ciclo operativo de cinco fases: PHVA (Planificar, Hacer, Verificar, Actuar), basado en la norma ISO 27001:2013. Estas fases permiten al ICANH gestionar adecuadamente la seguridad y privacidad de sus activos de información.

5.1 PLANEACIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

En la actualidad, y conforme con lo establecido en el título 9 del Decreto Único Reglamentario 1078 de 2015 del sector de Tecnologías de la Información y las Comunicaciones, el ICANH trabaja de forma continua para implementar el Modelo de Seguridad y Privacidad de la Información (MSPI) como parte de la Estrategia de Gobierno Digital. El objetivo principal es preservar la integridad, confidencialidad, disponibilidad y privacidad de la información, mediante la adecuada gestión del riesgo, la aplicación de normativas vigentes y la implementación de mejores prácticas en cuanto a seguridad de la información.

El MSPI está basado en el ciclo de mejoramiento continuo PHVA (Planear, Hacer, Verificar, Actuar), lo cual asegura que el modelo esté sujeto a revisiones constantes cada vez que haya cambios significativos en la infraestructura o cuando sea necesario mejorar su efectividad con base en mediciones de parámetros clave en su operación. Este ciclo permite establecer, implementar, operar, supervisar, revisar, mantener y mejorar el modelo de seguridad y privacidad de la información.

A continuación, se detallan los componentes de cada fase del ciclo:

Ilustración 1. Fases del ciclo PHVA.

5.2 DIAGNÓSTICO Y AUTODIAGNÓSTICO

El ICANH, como entidad pública nacional adscrita al Ministerio de las Culturas, las Artes y los Saberes, debe cumplir con las metas de Seguridad de la Información establecidas por MINTIC. Para estructurar el contexto, realizar el análisis e implementar las acciones necesarias, se utilizaron herramientas de diagnóstico proporcionadas por los entes rectores, siguiendo los lineamientos para la apropiación de la estrategia de Gobierno Digital. Con el fin de identificar el nivel de madurez del ICANH en cuanto a la seguridad y privacidad de la información, se utilizó la herramienta “Instrumento de Evaluación MSPI de MINTIC”, obteniendo en la vigencia 2024 el siguiente resultado:

No.	EVALUACIÓN DE EFECTIVIDAD DE CONTROLES			
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	100	100	OPTIMIZADO
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	89	100	OPTIMIZADO
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	69	100	GESTIONADO
A.8	GESTIÓN DE ACTIVOS	83	100	OPTIMIZADO
A.9	CONTROL DE ACCESO	93	100	OPTIMIZADO
A.10	CRIPTOGRAFÍA	100	100	OPTIMIZADO
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	77	100	GESTIONADO
A.12	SEGURIDAD DE LAS OPERACIONES	87	100	OPTIMIZADO
A.13	SEGURIDAD DE LAS COMUNICACIONES	82	100	OPTIMIZADO
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	83	100	OPTIMIZADO
A.15	RELACIONES CON LOS PROVEEDORES	40	100	REPETIBLE
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	80	100	GESTIONADO
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	84	100	OPTIMIZADO
A.18	CUMPLIMIENTO	88.5	100	OPTIMIZADO
PROMEDIO EVALUACIÓN DE CONTROLES		**83**	**100**	**OPTIMIZADO**

Tabla 1. Resultados efectividad de controles.

Ilustración 2. Elaboración propia, adaptado del instrumento MSPI de MINTIC.

La evaluación de los controles de seguridad en el ICANH muestra un promedio del 83% en la evaluación de los controles de la norma ISO 27001, lo que indica que los procesos y controles están adecuadamente documentados y comunicados. Sin embargo, algunos dominios de la norma requieren fortalecerse para cumplir con los estándares internacionales de seguridad. Este fortalecimiento es clave para asegurar el cumplimiento del Modelo de Seguridad y Privacidad del MINTIC, alinearse con el Modelo Integrado de Planeación y Gestión (MIPG) y cumplir con la política de Gobierno Digital. Además, es necesario seguir un proceso sistemático de evaluación y mejora continua, según la metodología del MINTIC, para incrementar el nivel de madurez del Sistema de Gestión de Seguridad de la Información.

6. ESTRATEGIA DE SEGURIDAD DIGITAL

El Instituto Colombiano de Antropología e Historia define una estrategia integral de Seguridad de la Información, que abarca principios, políticas, procedimientos, guías, manuales, formatos y directrices orientadas a la gestión adecuada de la seguridad de la información. Esta estrategia se fundamenta en la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI), como eje central.

En este contexto, el Instituto adopta las cinco estrategias específicas propuestas por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), con el fin de conformar una estrategia general de seguridad digital sólida y coherente:

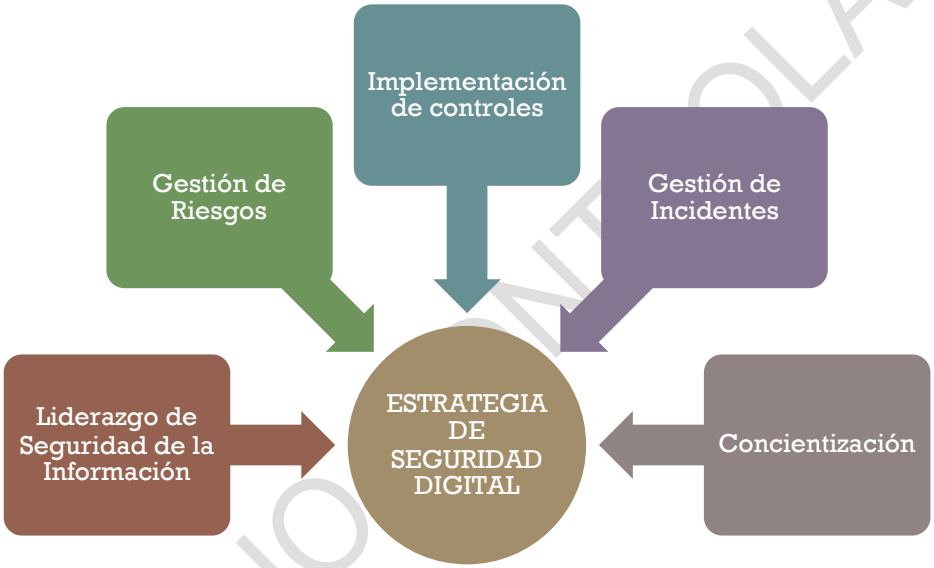

Ilustración 3. Estrategias de Seguridad Digital (Fuente: MinTIC).

6.1 DESCRIPCIÓN DE LAS ESTRATEGIAS ESPECÍFICAS (EJES)

A continuación, se describe el objetivo de cada una de las estrategias específicas a implementar, alineando las actividades con lo descrito el MPSI y la resolución 500 de 2021:

ESTRATEGIA / EJE	DESCRIPCIÓN/OBJETIVO
Liderazgo de seguridad de la información	Asegurar que se establezca el Modelo de Seguridad y Privacidad de la Información (MSPI) a través de la aprobación de la política general y demás lineamientos que se definan buscando proteger la confidencialidad, integridad y disponibilidad de la información teniendo como pilar fundamental el compromiso de la alta dirección y de los líderes de las diferentes dependencias y/o procesos de la Entidad a través del establecimiento de los roles y responsabilidades en seguridad de la información.
Gestión de riesgos	Determinar los riesgos de seguridad de la información a través de la planificación y valoración que se defina buscando prevenir o reducir los efectos indeseados teniendo como pilar fundamental la implementación de controles de seguridad para el tratamiento de los riesgos.
Implementación de controles	Planificar e implementar las acciones necesarias para lograr los objetivos de seguridad y privacidad de la información y mantener la confianza en la ejecución de los procesos de la Entidad, se pueden subdividir en controles tecnológicos y/o administrativos.
Gestión de Incidentes	Garantizar una administración de incidentes de seguridad de la información con base a un enfoque de integración, análisis, comunicación de los eventos e incidentes y las debilidades de seguridad en pro de conocerlos y resolverlos para minimizar el impacto negativo de estos en la Entidad.
Concientización	Fortalecer la construcción de la cultura organizacional con base en la seguridad de la información para que convierta en un hábito, promoviendo las políticas, procedimientos, normas, buenas prácticas y demás lineamientos, la transferencia de conocimiento, la asignación y divulgación de responsabilidades de todo el personal de la entidad en seguridad y privacidad de la información.

Tabla 2. Ejes Estrategia de Seguridad Digital.

6.2 PORTAFOLIO DE PROYECTOS / ACTIVIDADES

Para cada estrategia específica, El Instituto Colombiano de Antropología e Historia (ICANH) define los siguientes proyectos y productos esperados, que tienen por objetivo lograr la implementación y mejoramiento continuo del Sistema de Gestión de Seguridad de la Información (SGSI):

ESTRATEGIA / EJE	PROYECTO	PRODUCTOS ESPERADO
Liderazgo de seguridad de la información	PROYECTO 1: Establecer el Plan Estratégico de Seguridad de la Información. PROYECTO 2: Revisar y actualizar la Política General de Seguridad de la Información PROYECTO 3: Capacitar en seguridad de la información a los roles de seguridad de la información de la entidad. PROYECTO 4: Desarrollar e implementar una política de continuidad del negocio.	• Plan Estratégico de Seguridad de la Información establecido y aprobado por el Comité de desempeño Institucional. • Política General de Seguridad de la Información actualizada y aprobada por el Comité de desempeño Institucional. • Elaboración de documentos de apoyo para capacitación a funcionarios, actas de capacitación o evidencia de participación en las capacitaciones. • Política de continuidad de negocios.
Gestión de riesgos	PROYECTO 1: Gestión de riesgos y planes de tratamiento de riesgos de seguridad de la información PROYECTO 2: Definir planes de tratamiento de riesgos de seguridad. PROYECTO 3: Identificar, valorar y clasificar riesgos asociados a continuidad del negocio.	• Informes de seguimiento a de riesgos de seguridad de la información • Definir planes de tratamiento de riesgos • Matriz de riesgos de la Información.
Concientización	PROYECTO 1: Desarrollo de actividades de uso y apropiación del Modelo de Seguridad y Privacidad de la Información. PROYECTO 2: Formular el Plan de Comunicación y Sensibilización en Seguridad de la Información.	• Plan de capacitación y socialización de seguridad y privacidad de la información • Evidencias de las capacitaciones y socialización realizadas. • Plan de Comunicación y Sensibilización en Seguridad de la Información debidamente establecido y aprobado por el Comité de desempeño Institucional.
Implementación de controles	PROYECTO 1: Realizar seguimiento y actualización del Instrumento de Evaluación ISO:27001 y MSPI implementado en la entidad. PROYECTO 2: Análisis de pruebas vulnerabilidades de la red. PROYECTO 3: Política de respaldos de información. PROYECTO 4: Renovación de licenciamiento y soporte de infraestructura de seguridad Perimetral (Firewalls y software de Antivirus).	• Actualización del MSPI Instrumento de Evaluación ISO:27001 y MSPI. • Política de respaldos de información. • Informes del estado de la red, con respecto al nivel de seguridad informática. • Infraestructura de seguridad debidamente asegurada con soporte y licencia durante la vigencia siguiente.

Gestión de incidentes	PROYECTO 1: Actualizar el procedimiento de Gestión de Incidentes de seguridad de la información, adaptándolo a las necesidades de la entidad. PROYECTO 2: Capacitar al personal en la gestión de incidentes de seguridad de la información. PROYECTO 3: Gestionar, documentar los incidentes de seguridad de la información escalados al Área de TI.	• Procedimiento y manual de gestión de incidentes de seguridad de la información. • Evidencias de las sesiones de capacitación desarrolladas. • Informes periódicos sobre los incidentes de seguridad de la información gestionados por el Área de TI.

Tabla 3. Portafolio de proyectos y operaciones del Plan Estratégico de Seguridad de la Información (PESI).

6.3 CRONOGRAMA DE ACTIVIDADES / PROYECTOS:

El responsable de seguridad de la información, con base a los proyectos definidos en la sección anterior, deberá establecer un cronograma de actividades donde se evidencie como se llevarán a cabo cada uno de los proyectos previstos. Las actividades podrán desarrollarse de forma secuencial o paralela según se considere.

Acción	Descripción	Actividades programadas	Fechas límite												Fecha inicial	Fecha final	Nombre del registro / evidencia
			Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic			
Desarrollo de la norma ISO/IEC 27001:2013, Matriz de Aplicabilidad.	Actualización de los controles de seguridad establecidos en la MATRIZ DE APLICABILIDAD ISO/IEC 27001:2013.	1.1. Realizar análisis de la matriz de aplicabilidad 2024. 1.2 Realizar la actualización matriz de aplicabilidad.	**1.1**						**1.2**						2/02/2025	30/07/2025	1.1. Documento de análisis de la matriz de aplicabilidad 2024. 1.2. Matriz de aplicabilidad 2025.
Actualización Activos de Información	Actualización de la Matriz de Activos críticos de información.	2.1 Reuniones con Subdirecciones y Secretaría General para actualización de activos críticos de información. 2.2 Actualización matriz de activos críticos de información.			**2.1**				**2.2**						2/03/2025	30/09/2025	2.1. Cuatro actas de reunión con subdirecciones y Secretaría General. 2.2. Matriz de activos críticos de información 2025.
Actualización Matriz de Riesgos	Actualización del documento Matriz de Riesgos de información.	3.1. Realizar análisis de la matriz de riesgos de información 2024. 3.2 Actualizar la matriz de riesgos de información.			**3.1**			**3.2**							2/03/2025	30/08/2025	3.1. Documento de análisis de la matriz de riesgos de información 2024. 3.2. Matriz de riesgos de información 2025.

Acción	Descripción	Actividades programadas	Fechas límite												Fecha inicial	Fecha final	Nombre del registro / evidencia
			Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic			
Sensibilización y Capacitación en Seguridad de la Información	Realizar de manera trimestral campañas y/o sesiones de socialización y sensibilización sobre las políticas de seguridad y privacidad de la información, dirigidas específicamente a los funcionarios y contratistas del ICANH.	4.1 Construir el plan de campañas y sensibilización sobre políticas de seguridad y privacidad de la información. 4.2. Implementar el plan de campañas y sensibilización sobre políticas de seguridad y privacidad de la información.	**4.1**		**4.2**										2/01/2025	30/12/2025	4.1. Documento Plan de campañas y sensibilización sobre políticas de seguridad y privacidad de la información. 4.2. 4 informes de la implementación del Plan de campañas y sensibilización sobre políticas de seguridad y privacidad de la información.
Realizar pruebas de vulnerabilidad y Ethical Hacking a la red institucional	Realizar dos evaluaciones con periocidad semestral al estado de la red, con respecto al nivel de seguridad informática.	5.1 Implementar en el primer semestre 2025 una (1) evaluación sobre el estado de la red, con respecto al nivel de seguridad informática. 5.2 Implementar en el segundo semestre 2025 una (1) evaluación sobre el estado de la red, con respecto al nivel de seguridad informática.	**5.1**						**5.2**						2/01/2025	30/12/2025	5.1. Informe del estado de red, con respecto al nivel de seguridad informática primer semestre 2025. 5.2. Informe del estado de red, con respecto al nivel de seguridad informática segundo semestre 2025.

Acción	Descripción	Actividades programadas	Fechas límite												Fecha inicial	Fecha final	Nombre del registro / evidencia
			Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic			
Actualización Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información	Revisión y actualización del documento Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.	6.1. Realizar análisis del documento Tratamiento de Riesgos de Seguridad y Privacidad de la Información. 6.2 Realizar la actualización del documento de Tratamiento de Riesgos y Privacidad de la Información.		**6.1**			**6.2**								2/02/2025	30/08/2025	6.1. Documento de análisis del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información. 6.2. Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información 2025.
Gestionar los incidentes de Seguridad y Privacidad de la Información	Realizar informes de los incidentes de seguridad de la información, y socializar al comité de gestión y desempeño para tomar medidas preventivas y correctivas.	7. 1. Consolidar Trimestralmente un informe de los incidentes de seguridad de la información 7.2. Socializar semestralmente al Comité de Gestión y Desempeño el informe de Incidentes de Seguridad de la Información.	**7.1**												2/01/2025	30/12/2025	7.1. Cuatro informes de incidentes de seguridad de la información. 7.2. Dos actas de socialización al comité de gestión de incidentes de seguridad de la información.
			7.2														


2-41
2-41
LIBRERIA
INSTITUTO COLOMBIANO DE
ANTROPOLOGIA E HISTORIA

Según la proyección de la PAA, las adquisiciones siguientes forman parte de las medidas de control destinadas a fortalecer el sistema de seguridad y protección de la información.

DESCRIPCIÓN DEL OBJETO CONTRACTUAL	VALOR ESTIMADO MENSUAL	VALOR ESTIMADO ANUAL
Adquirir la renovación de las licencias del equipo de seguridad perimetral y antivirus, renovación del pool de direcciones ipv6, y renovación de las licencias de los dispositivos Access Point para el Instituto Colombiano de Antropología e Historia.	$ 220.000.000	$ 220.000.000,00
Prestar servicios profesionales con plena autonomía técnica, administrativa y financiera para la actualización, seguimiento, uso y apropiación del PETIC, SGSI y plan de comunicaciones TI del ICANH.	$ 4.897.200	$56.317.800
	Total	**$276.317.800,00**

7. RESPONSABLES

Respecto al Plan Estratégico de Seguridad de la Información (PESI), se definen los siguientes responsables:

ROL	RESPONSABILIDADES
Comité Institucional de Gestión de Desempeño	• Revisar y aprobar el Plan Estratégico de Seguridad de la Información (PESI).
Oficial de Seguridad de la Información	• Implementar las actividades y controles relevantes para la seguridad de la información. • Realizar seguimiento a las actividades establecidas en el PESI.
Área Funcional de Tecnologías de la Información y las Comunicaciones	• Implementar las actividades pertinentes al PESI. • Apoyar al Oficial de Seguridad de la Información en el despliegue y administración de soluciones tecnológicas de seguridad para proteger los activos del ICANH.
Funcionarios y Contratistas	• Implementación de políticas, lineamientos, procedimientos y controles de seguridad establecidos por la entidad.

8. BIBLIOGRAFÍA

- Manual de Gobierno Digital – MinTIC.
- https://www.mintic.gov.co/portal/inicio/Atencion-y-Servicio-a-la-Ciudadania/Transparencia/135830:Plan-de-seguridad-y-privacidad-de-la-informacion
- https://gobiernodigital.mintic.gov.co/portal/Manual-de-Gobierno-Digital/272948:Plan-Estrategico-de-Seguridad-de-la-Informacion-PESI
- https://www.normaiso27001.es/

CONTROL DE CAMBIOS

CONTROL DE CAMBIOS		
Versión	**Fecha**	**Descripción general del cambio**
01	2025-01-21	Aprobación del documento por parte del Comité Institucional de Gestión de Desempeño.

ELABORÓ	REVISÓ	APROBÓ
Cargo: Profesional Especializado Área de Tecnologías de la Información.	**Cargo:** Asesor Área de Tecnologías de la Información. Miembros del Comité Institucional de Gestión y Desempeño.	**Cargo:** Miembros del Comité Institucional de Gestión y Desempeño.
Fecha: 2025-01-14	**Fecha: 2025-01-20**	**Fecha: 2025-01-21**