PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN (PESI).

2026

Culturas

ICANH

Alhena Caicedo Fernández
Directora General

Jonathan Andrés Sánchez Corredor
Jefe de la Oficina de Tecnologías

ENERO DE 2026

Contenido

Tabla de Ilustraciones

Contenido de Tablas

1. 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.

2. Marco normativo

El Plan Estratégico de Seguridad de la Información (PESI) constituye el instrumento de planeación mediante el cual la entidad define la hoja de ruta para la protección de sus activos de información, la gestión de los riesgos de seguridad de la información y el fortalecimiento del Sistema de Gestión de Seguridad de la Información (SGSI).

La formulación e implementación del PESI es obligatoria para las entidades públicas, en la medida en que se deriva del cumplimiento de la Política de Gobierno Digital y del Modelo de Seguridad y Privacidad de la Información (MSPI), los cuales tienen sustento jurídico en el Decreto 1078 de 2015, que faculta al Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) para establecer modelos y lineamientos de obligatorio cumplimiento en materia de seguridad de la información.

En este contexto, el PESI se formula como un instrumento estratégico del MSPI, alineado con la Política Nacional de Seguridad Digital, los cuales se adoptan como referentes técnicos y buenas prácticas.

Norma	Descripción
Constitución Política de Colombia (Art. 15 y 74)	Fundamenta la necesidad del PESI para garantizar la protección de la información, los datos personales y el acceso responsable a la información pública.
Ley 1581 de 2012	Obliga a definir medidas estratégicas y planes de acción en el PESI para asegurar la confidencialidad, integridad y disponibilidad de los datos personales.
Ley 1712 de 2014	Exige que el PESI contemple controles que garanticen la seguridad de la información pública sin afectar la transparencia y el acceso a la información.
Decreto 1078 de 2015	Establece la obligatoriedad de implementar los lineamientos de seguridad de la información definidos por MinTIC, de los cuales se deriva la formulación del PESI como instrumento estratégico del MSPI.
Decreto 1499 de 2017 (MIPG)	Integra el PESI dentro de la planeación institucional, la gestión del riesgo y el control interno, asegurando su alineación con el PEI, el PETI y los planes institucionales.
CONPES 3854 de 2016	Orienta el enfoque del PESI hacia la gestión del riesgo digital y la protección de los activos estratégicos de información del Estado.
Modelo de Seguridad y Privacidad de la Información (MSPI – MinTIC)	Define al PESI como uno de los productos estratégicos del modelo, estableciendo su contenido, alcance y horizonte de planeación.
Guía para la Elaboración del PESI – MinTIC	Establece la estructura mínima, los componentes y la metodología para la formulación del PESI en las entidades públicas.
ISO/IEC 27001:2022	Referente técnico para estructurar las líneas estratégicas, objetivos y controles definidos en el PESI, sin carácter obligatorio.

Tabla 1. Marco normativo Plan Estratégico de Seguridad de la Información 2026

3. Objetivos

3.1. Objetivo general

Implementar el Plan Estrategico 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.

3.2. 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).

4. Alcance

Este documento presenta el Plan Estrategico 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.

5. 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.

6. Generalidades

El Plan Estratégico de Seguridad de la Información (PESI) de la entidad, establece los lineamientos estratégicos para la protección de los activos de información, en coherencia con la Política de Gobierno Digital, el Modelo de Seguridad y Privacidad de la Información (MSPI) y el Modelo Integrado de Planeación y Gestión (MIPG), garantizando el cumplimiento de la normatividad vigente y el apoyo al logro de los objetivos institucionales.

A continuación, se describen los principales elementos que caracterizan el PESI:

El PESI está dirigido a todos los usuarios que interactúan con los activos de información de la entidad, independientemente de su nivel jerárquico o modalidad de vinculación, incluyendo:

- Servidores públicos
- Contratistas y personal de apoyo
- Proveedores y terceros con acceso a información institucional
- Usuarios de los sistemas de información y servicios digitales

El PESI se articula con los principales instrumentos de planeación, gestión y control de la entidad, entre ellos:

- Plan Estratégico Institucional (PEI)
- Plan Estratégico de Tecnologías de la Información (PETI)
- Modelo Integrado de Planeación y Gestión (MIPG)

Así mismo se articula externamente con:

- Modelo Integrado de Planeación y Gestión (MIPG)
- Política de Gobierno Digital

7. Marco conceptual

7.1. Estado actual de la entidad respecto al SGSI

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.

7.2. Planeación del MSPI

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:

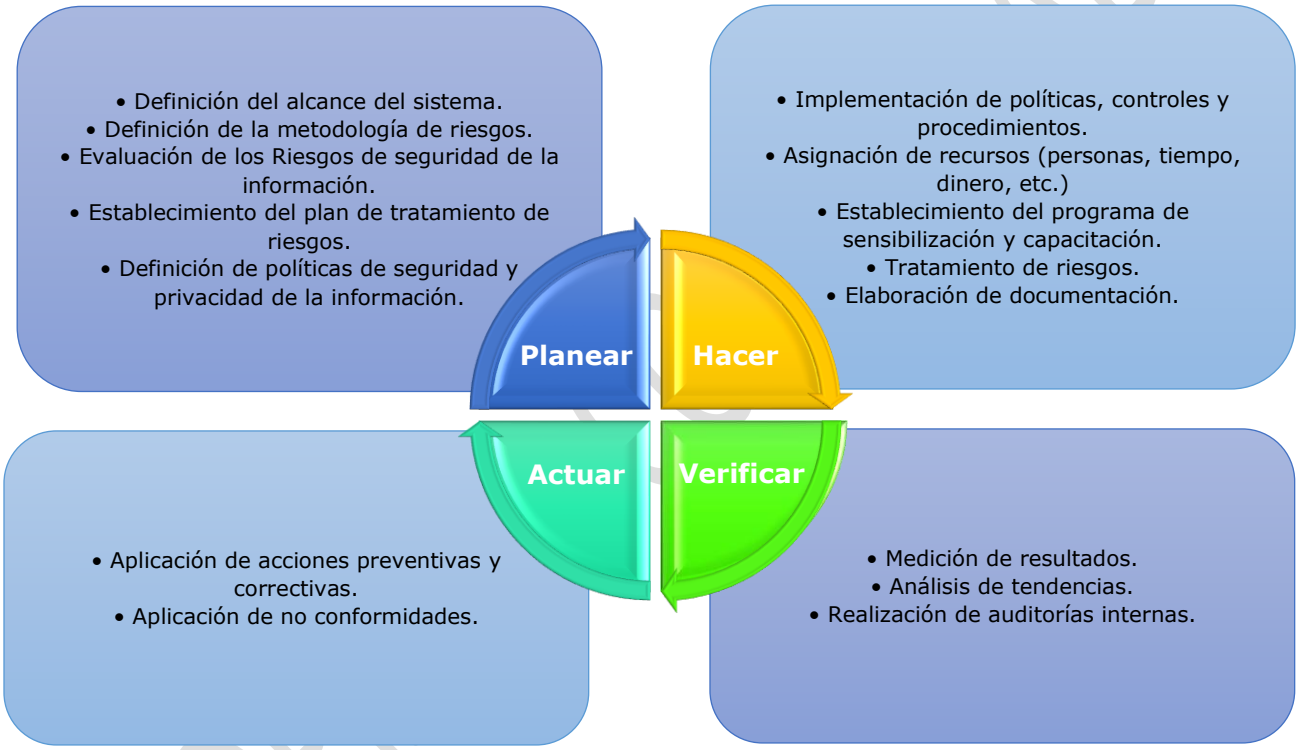

Ilustración 1. Fases del ciclo PHVA.

8. Diagnóstico y autodiagnóstico

El ICANH, en su calidad de entidad pública de orden nacional adscrita al Ministerio de las Culturas, las Artes y los Saberes, debe dar cumplimiento a las metas de Seguridad de la Información definidas por el Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC). Para la estructuración del contexto, el análisis y la implementación de las acciones correspondientes, se emplearon herramientas de autodiagnóstico suministradas por los entes rectores, en concordancia con los lineamientos para la apropiación de la estrategia de Gobierno Digital.

Con el propósito de identificar el nivel de madurez del ICANH en materia de seguridad y privacidad de la información, se aplicó la herramienta “Instrumento de Evaluación MSPI de MINTIC”, obteniendo para la vigencia 2025 el siguiente resultado:

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	Nivel de Madurez
A.5	CONTROLES ORGANIZACIONALES	81	100	**OPTIMIZADO**
A.6	CONTROLES DE PERSONAS	95	100	**OPTIMIZADO**
A.7	CONTROLES FÍSICOS	81	100	**OPTIMIZADO**
A.8	CONTROLES TECNOLÓGICOS	75	100	**GESTIONADO**
PROMEDIO EVALUACIÓN DE CONTROLES		**83**	**100**	**OPTIMIZADO**

Tabla 2. *Resultados efectividad de controles*

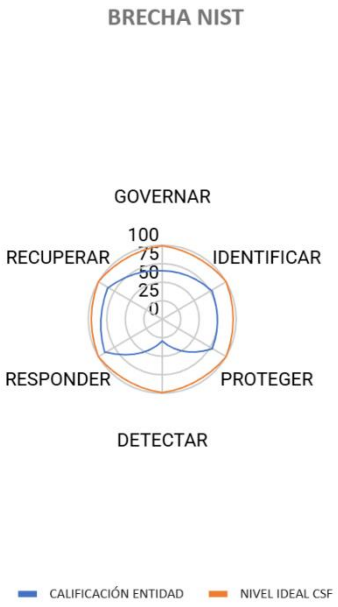

Ilustración 2. Adaptado del instrumento MSPI de MINTIC

El resultado obtenido evidencia que el ICANH dispone de un marco organizacional sólido para la gestión de la seguridad de la información, sustentado en la definición de políticas, procedimientos, roles y responsabilidades, así como en la alineación con la estrategia de Gobierno Digital y el Modelo de seguridad y Privacidad de la Información. Sin embargo, la brecha frente a la calificación objetivo (100) evidencia oportunidades de mejora relacionadas a la formalización, medición y fortalecimiento continuo de algunos controles, especialmente en la gestión del riesgo, la articulación transversal del SGSI y el robustecimiento de métricas e indicadores.

El estado actual del servicio de Seguridad de la Información del ICANH es consistente con una entidad que ha avanzado de manera estructurada en la implementación del SGSI, conforme a la ISO/IEC 27001:2022 y al Modelo de Seguridad y Privacidad de la Información de MINTIC. Las brechas identificadas no representan incumplimientos críticos, sino oportunidades de mejora orientadas a la optimización de controles tecnológicos, el fortalecimiento de capacidades de detección y respuesta, y la consolidación de un enfoque de mejora continua que permita alcanzar el nivel objetivo de madurez en todos los dominios evaluados.

9. 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:

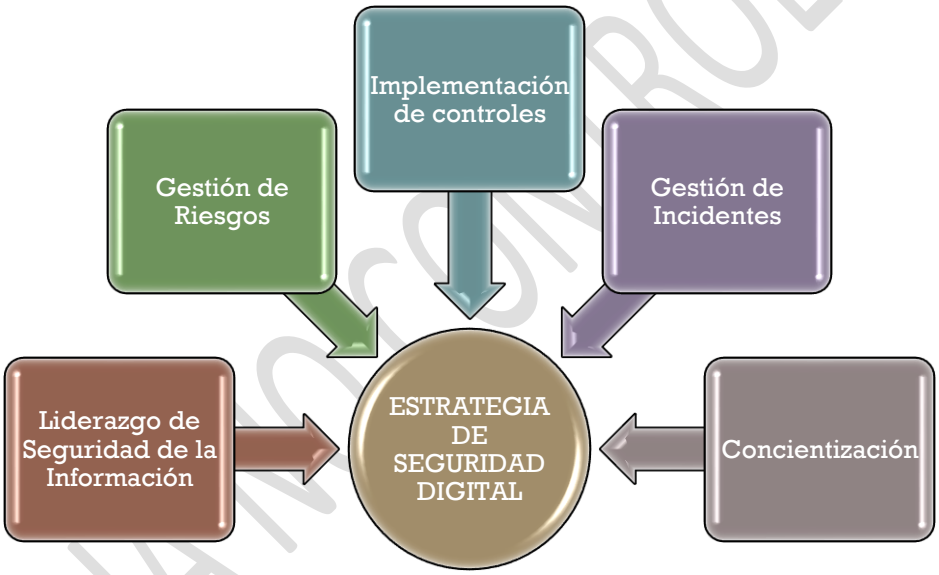

Ilustración 3. Estrategias de Seguridad Digital (Fuente: MinTIC).

10. 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 3. Ejes Estrategia de Seguridad Digital.

11. Resultados de la vigencia anterior

Durante la vigencia 2025, la entidad desarrolló acciones orientadas al fortalecimiento del Plan Estratégico de Seguridad de la Información (PESI), en concordancia con los lineamientos del Modelo Integrado de Planeación y Gestión (MIPG). En el componente de planeación y control, se elaboró la Matriz de Aplicabilidad 2025, lo cual permitió evaluar el nivel de implementación de los controles de seguridad de la información, identificar brechas y definir acciones de mejora alineadas con los riesgos institucionales y los objetivos estratégicos de la entidad.

Así mismo, se fortaleció la gestión de activos de información mediante la elaboración de la Matriz de Activos de Información, garantizando la identificación, clasificación y valoración de los activos críticos, en coherencia con el enfoque de gestión por procesos y la protección de la información como activo estratégico para la toma de decisiones y la prestación del servicio.

En materia de administración del riesgo, se estructuró la matriz de riesgos de información para la vigencia 2025 y se avanzó en la consolidación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, permitiendo identificar amenazas, vulnerabilidades e impactos sobre la confidencialidad, integridad y disponibilidad de la información, así como definir controles y planes de tratamiento con actividades acordes a los riesgos institucionales. Adicionalmente, se formuló y ejecutó el Plan de Campañas de Sensibilización en Seguridad y Privacidad de la Información, contribuyendo al fortalecimiento de la cultura organizacional, la apropiación de las políticas de seguridad de la información y la corresponsabilidad de los servidores públicos y contratistas.

Finalmente, se fortaleció el proceso de gestión de incidentes a través de la elaboración de informes de incidentes de seguridad de la información y del documento de socialización del proceso de gestión de incidentes, contribuyendo a mejorar la capacidad de detección, respuesta y aprendizaje organizacional frente a eventos que puedan afectar la confidencialidad, integridad y disponibilidad de la información.

a) Resultados del indicador asociado al plan institucional de la vigencia anterior.

12. Gestión Plan vigencia actual

a) Metodología

Para la vigencia actual, la implementación del Plan Estratégico de Seguridad y Privacidad de la Información (PESI) se desarrollará bajo un enfoque de gestión por procesos, administración del riesgo y mejora continua.

La metodología adoptada se fundamenta en las siguientes etapas:

1. Planeación: Se definen las acciones, responsables, recursos y tiempos para la ejecución de las actividades relacionadas con la seguridad de la información, priorizando aquellas orientadas a la disponibilidad, confidencialidad e integridad de los activos de información. Esta etapa incluye la programación de pruebas de restauración, actualización de activos de información, análisis de vulnerabilidades, actividades de sensibilización y gestión de incidentes.
2. Ejecución: Las actividades se desarrollan conforme al cronograma establecido. Durante esta fase se ejecutan pruebas semestrales de restauración de aplicaciones y sistemas críticos, se mantiene actualizado el inventario y clasificación de activos, se realizan análisis periódicos de vulnerabilidades, se implementan campañas de sensibilización y se gestionan los incidentes de seguridad de la información.
3. Verificación: Se realiza el seguimiento al cumplimiento de las actividades mediante la revisión de evidencias, informes técnicos y registros asociados a cada acción, permitiendo evaluar el nivel de avance, la efectividad de los controles implementados y la identificación de desviaciones o brechas.
4. Mejora continua: Con base en los resultados del seguimiento y la evaluación, se definen acciones de mejora orientadas al fortalecimiento del PESI, la reducción de riesgos y el incremento del nivel de madurez en seguridad y privacidad de la información.

b) Ejecución – Cronograma

El cronograma de ejecución de las actividades del PESI para la vigencia actual se encuentra alineado con el plan de acción institucional y se desarrolla de la siguiente manera:

ICANH	PROCEDIMIENTO FORMULACIÓN Y SEGUIMIENTO DE LA PLANEACIÓN INSTITUCIONAL	CÓDIGO:	DE-PR-02-FO-03
	FORMATO PLANES INSTITUCIONALES	VERSIÓN:	02
		FECHA:	11/12/2025

No.	Actividad	Descripción	Nombre del responsable	Cargo responsable	Mes de ejecución												Fecha inicia	Fecha final	Evidencia de la actividad
					Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic			
1	Ejecución de pruebas semestrales de restauración de aplicaciones y sistemas de información.	Realizar pruebas semestrales de restauración de aplicaciones y sistemas de información críticos del ICANH para verificar la efectividad de los respaldos y la capacidad de recuperación ante incidentes de seguridad o eventos disruptivos.	Oficial Seguridad de la Información	Oficial Seguridad de la Información						X						X	2/02/2026	30/12/2026	Informe semestral de pruebas de restauración de sistemas y aplicaciones críticas
2	Actualización de Activos de Información	Actualizar el inventario institucional de activos de información ante novedades como cambios en los procesos, incorporación de nuevos activos, ajustes en su clasificación (confidencialidad, integridad y disponibilidad) o cambios y migraciones de los sistemas donde se almacenan.	Oficial Seguridad de la Información	Oficial Seguridad de la Información											X		9/03/2026	30/11/2026	Matriz de activos de información actualizada - 2026
3	Análisis de vulnerabilidades de infraestructura tecnológica	Realizar análisis periódicos de vulnerabilidades sobre la infraestructura tecnológica del ICANH para identificar, evaluar y priorizar debilidades de seguridad en servidores, redes, dispositivos y sistemas de información, y establecer acciones de mitigación orientadas a reducir el riesgo de incidentes de seguridad de la información.	Oficial Seguridad de la Información	Oficial Seguridad de la Información			X			X			X			X	2/02/2026	30/12/2026	Informe trimestral de análisis de vulnerabilidades de la infraestructura tecnológica
4	Sensibilización y capacitación sobre seguridad de la información al personal	Diseñar e implementar actividades de sensibilización en seguridad de la información dirigidas al personal del ICANH, con el fin de fortalecer la cultura de seguridad y promover buenas prácticas para el manejo adecuado y seguro de la información.	Oficial Seguridad de la Información	Oficial Seguridad de la Información			X			X			X			X	2/02/2026	30/12/2026	Registro consolidado de sensibilización y capacitación en seguridad de la información
5	Gestión de incidentes de Seguridad de la Información	Gestionar los incidentes de seguridad de la información identificados en el ICANH, asegurando su registro, clasificación, atención oportuna, escalamiento cuando aplique y cierre, con el fin de reducir su impacto y fortalecer la mejora continua.	Oficial Seguridad de la Información	Oficial Seguridad de la Información			X			X			X			X	2/02/2026	30/12/2026	Informe trimestral de gestión de incidentes de seguridad de la información
				Total actividades planeadas por mes	0	0	3	0	0	4	0	0	3	0	1	4			
				Total actividades planeadas por trimestre	3			4			3			5					

Ilustración 4. Cronograma de actividades PESI 2026

c) Seguimiento y evaluación

El seguimiento del Plan Estratégico de Seguridad de la Información para la vigencia actual se realizará de manera periódica para medir el avance de las actividades programadas. Como mecanismo principal de medición, se establece el siguiente indicador de eficacia, orientado a evaluar la implementación y gestión del PESI:

- Indicador: Implementación y gestión del PESI.
- Objetivo del indicador: Establecer el grado de cumplimiento de las actividades definidas en el PSPI, específicamente las relacionadas con los Planes de Tratamiento de Riesgos de Seguridad y Privacidad de la Información y las acciones de Seguridad y Privacidad de la Información.
- Tipo de indicador: Eficacia
- Fórmula: (# actividades cumplidas / # actividades planeadas) x 100
  Acumulado
- Unidad de medida: Porcentaje
- Periodicidad de medición: Acumulado durante la vigencia
- Responsable del seguimiento: Oficial de Seguridad de la Información

El resultado del indicador se consolidará con base en la verificación de evidencias asociadas a cada actividad, tales como informes técnicos, matrices actualizadas, registros de sensibilización, reportes de incidentes y demás documentos que soporten su ejecución. Este seguimiento permitirá identificar oportunamente desviaciones frente a lo planeado, definir acciones correctivas y de mejora; Se realizará seguimiento interno trimestral a cargo del Oficial de Seguridad de la Información y la Oficina de Tecnologías, y seguimiento institucional por parte de la Oficina Asesora de Planeación. Los resultados se consolidarán en la matriz institucional de planes y se reportarán conforme al calendario institucional.

13. 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.

Tabla 4. Responsabilidades de la implementación del PESI

Control de cambios		
Versión	**Fecha**	**Descripción general del cambio**
01	2024-12-30	Creación de documento
02	2026-01-26	Actualización y ajuste integral del documento para la vigencia 2026

LABORÓ	REVISÓ	APROBÓ
Cargo: Profesional Especializado Oficina de Tecnologías	**Cargo:** Asesor de Oficina de Tecnologías Contratista Oficina Asesora de Planeación	**Cargo:** Jefe de la Oficina de Tecnologías
Fecha: 30-12-2024	**Fecha: 30-12-2024**	**Fecha: 29-01-2025**