Realización de Fases de implementación del Modelo de Seguridad y Privacidad de la Información del Instituto Nacional de Salud conforme a los lineamientos del Ministerio de Tecnologías de la Información y las Comunicaciones y la Estrategia de Gobierno en Línea.

CONTROL DE CAMBIOS

Av. Calle 26 No. 51- 20, Bogotá, D.C., Colombia
Conmutador: (1) 220 7700 Ext. 1703-1704
fax: 220 7700 Ext. 1283-1269
correo electrónico: contactenos@ins.gov.co
Página web: **www.ins.gov.co**
Línea gratuita nacional: 018000 113 400

Fecha de Actualización	Versión	Creado Por:	Aprobado por:
12/12/2018	**1.1**	**Joaquín Afanador**	**Elsa Baracaldo**

Av. Calle 26 No. 51- 20, Bogotá, D.C., Colombia
Conmutador: (1) 220 7700 Ext. 1703-1704
fax: 220 7700 Ext. 1283-1269
correo electrónico: contactenos@ins.gov.co
Página web: **www.ins.gov.co**
Línea gratuita nacional: 018000 113 400

TABLA DE CONTENIDO

Av. Calle 26 No. 51- 20, Bogotá, D.C., Colombia
Conmutador: (1) 220 7700 Ext. 1703-1704
fax: 220 7700 Ext. 1283-1269
correo electrónico: contactenos@ins.gov.co
Página web: **www.ins.gov.co**
Línea gratuita nacional: 018000 113 400

1. INTRODUCCIÓN

Este documento tiene como fin presentar una hoja de ruta de proyectos, que permitirán el establecimiento, implementación, operación, monitoreo, revisión y mejora continua del Sistema de Gestión de Seguridad y Privacidad de la Información en los que el Instituto Nacional de Salud se encuentra trabajando actualmente con el apoyo de este proyecto de consultoría.

Esto demuestra que la entidad se encuentra comprometida con la seguridad y privacidad de la información, asignando los recursos necesarios para garantizar que los procesos de la entidad se encuentren incluidos en el alcance de dichos sistemas, permitiéndole a la entidad dar cumplimiento a sus objetivos estratégicos.

2. OBJETIVO GENERAL

Establecer el PESI a través de un plan de ruta de proyectos a tres (3) años para el establecimiento, implementación, operación, monitoreo, revisión y mejora continua del Sistema de Gestión de Seguridad y Privacidad de la Información en el INS.

2.1. Objetivos Específicos

- Presentar los proyectos a realizar como parte del PESI, incluyendo descripción, alcance, prioridad, costo y tiempos aproximados.
- Presentar la alineación de los proyectos presentados con la estrategia del INS, mediante la asociación de los objetivos de seguridad y los planes de tratamiento de riesgos (si aplica).

Av. Calle 26 No. 51- 20, Bogotá, D.C., Colombia
Conmutador: (1) 220 7700 Ext. 1703-1704
fax: 220 7700 Ext. 1283-1269
correo electrónico: contactenos@ins.gov.co
Página web: www.ins.gov.co
Línea gratuita nacional: 018000 113 400

3. PLAN DE RUTA DE PROYECTOS

Los planes estratégicos para el Sistema de Gestión de Seguridad y Privacidad de la Información en el INS, se desarrollan con base en los siguientes documentos:

- Informe de análisis de brechas ISO 27001.
- Informe de Diagnostico de Protección de Datos Personales.
- Diagnóstico mediante instrumento de evaluación de MSPI.
- Análisis de vulnerabilidades a la infraestructura de la Organización.
- Informe de análisis de Riesgo
- Planes de Tratamiento de Riesgo

La ejecución de estos planes se planifica entre los años 2019 y 2021, de acuerdo a su prioridad (basada en la cantidad de riesgos que trata) y a las buenas prácticas de seguridad de la información.

3.1. Proyectos estratégicos

Prioridad	1
Nombre	Fase II – Implementación del Sistema de Gestión de Seguridad de la Información
Descripción	Continuidad en la implementación del SGSI mediante una serie de actividades solicitadas por la norma ISO 27001 y el MSPI.
Alcance	• Acompañamiento en la implementación de políticas, procedimientos y controles. • Seguimiento en la implementación de planes de tratamiento de riesgos • Seguimiento a la ejecución del PESI • Acompañamiento en la implementación de los planes de cierre de brechas • Diseño, desarrollo y ejecución del plan implementación del plan de capacitación y sensibilización (incluye capacitación a responsables de riesgos) • Medición de indicadores y definición de acciones correctivas • Participación en los comités de seguridad y privacidad • Actualización de inventario de activos de información y bases de datos personales • Ejecución y actualización del análisis de riesgos y planes de tratamiento • Ejecución de auditoría y seguimiento al cierre de los hallazgos de auditorías anteriores • Pruebas semestrales de ejecución de análisis de vulnerabilidades y Ethical hacking • Actualización anual de la documentación del sistema de gestión de seguridad de acuerdo a lo solicitado por la norma • Acompañamiento en la revisión gerencial del sistema y definición de acciones de mejora • Medición del nivel de madurez del sistema • Definición de proyectos de fortalecimiento del SGSI

Av. Calle 26 No. 51- 20, Bogotá, D.C., Colombia
Conmutador: (1) 220 7700 Ext. 1703-1704
fax: 220 7700 Ext. 1283-1269
correo electrónico: contactenos@ins.gov.co
Página web: www.ins.gov.co
Línea gratuita nacional: 018000 113 400

	• Auditoría de cumplimiento de la ley 1581 de 2012 y protección de datos personales, desde la perspectiva de responsabilidad demostrada
Costo aproximado	$ 600.000.000 más IVA
Objetivos de seguridad relacionados	• Proteger, preservar y administrar los activos de información, las bases de datos personales y las tecnologías utilizadas para su procesamiento, frente a amenazas internas o externas, con el fin de asegurar la confidencialidad, la integridad y disponibilidad, de manera coordinada con las partes involucradas. • Aplicar un proceso de gestión de riesgos de seguridad de la información y bases de datos personales, mediante la ejecución de medidas apropiadas con el fin de identificar, analizar, evaluar, tratar y mitigar los riesgos y así reducir el impacto potencial a niveles aceptables sobre los riesgos asociados con la pérdida de la confidencialidad, de integridad y de disponibilidad. • Implementar, operar y revisar periódicamente los controles establecidos en la declaración de aplicabilidad, para la prevención y mitigación de los riesgos de seguridad de la información. • Disponer de medidas para atender oportunamente eventos de seguridad de la información con el fin de disminuir los impactos negativos ocasionados por los incidentes de Seguridad de la Información, que se puedan llegar a presentar en la Entidad. • Establecer las acciones necesarias, para asegurar la mejora continua del Sistema de Seguridad de la Información y Protección de Datos Personales. • Fortalecer la cultura de seguridad de la información en la Entidad, a través de la gestión del conocimiento de seguridad de la información.
Planes de tratamiento de riesgo relacionados	• PT029 • PT026 • PT048 • PT009 • PT028 • PT007 • PT013 • PT014 • PT016 • PT049 • PT020 • PT012 • PT002 • PT032 • PT027 • PT023 Ver detalle de estos planes en el documento “Plan de tratamiento de riesgos seguridad INS.xlsx entregado por IT Security Services como parte de la consultoría”.
Tiempo estimado de ejecución	10 meses

Prioridad	2
Nombre	Implementación de Prevención de Fuga de Información (DLP)
Descripción	Implementación de una solución que permita la fuga o extracción de información sensible del INS
Alcance	Contratar un tercero especializado que permita lograr el monitoreo y/o bloqueo de salida de información del INS a través de:

Av. Calle 26 No. 51- 20, Bogotá, D.C., Colombia
Conmutador: (1) 220 7700 Ext. 1703-1704
fax: 220 7700 Ext. 1283-1269
correo electrónico: contactenos@ins.gov.co
Página web: **www.ins.gov.co**
Línea gratuita nacional: 018000 113 400

	• Puertos USB • Correo electrónico • Servicios de red (Internet, red local) El tercero debe garantizar: • Dimensionamiento de la solución • Implementación • Operación y soporte
Costo aproximado	$ 135.000.000 más IVA
Objetivos de seguridad relacionados	• Proteger, preservar y administrar los activos de información, las bases de datos personales y las tecnologías utilizadas para su procesamiento, frente a amenazas internas o externas, con el fin de asegurar la confidencialidad, la integridad y disponibilidad, de manera coordinada con las partes involucradas. • Implementar, operar y revisar periódicamente los controles establecidos en la declaración de aplicabilidad, para la prevención y mitigación de los riesgos de seguridad de la información. • Disponer de medidas para atender oportunamente eventos de seguridad de la información con el fin de disminuir los impactos negativos ocasionados por los incidentes de Seguridad de la Información, que se puedan llegar a presentar en la Entidad. • Adopción de Responsabilidad Demostrada con el fin de reducir la probabilidad de violación de la privacidad de los datos personales en de la Entidad.
Planes de tratamiento de riesgo relacionados	• PT015 Ver detalle de estos planes en el documento “Plan de tratamiento de riesgos seguridad INS.xlsx entregado por IT Security Services como parte de la consultoría”.
Tiempo estimado de ejecución	Anual, permanente.

Prioridad	3
Nombre	Aseguramiento de la plataforma tecnológica y remediación de vulnerabilidades
Descripción	Servicio de aseguramiento y remediación de las vulnerabilidades identificadas en los escaneos periódicos y en los informes de hacking ético.
Alcance	• Desarrollo de guías de aseguramiento y procedimientos de remediación de vulnerabilidades para todo el software base del INS, entre ellos: sistemas operativos, dispositivos de red, soluciones de seguridad, motores de bases de datos y servidores WEB. • Aplicación de las guías de aseguramiento y remediación de vulnerabilidades en ambientes pre productivos (desarrollo, pruebas, calidad, entrenamiento, etc.) • Registro en CMDB, apoyo en gestión de cambios, gestión de relación interna, casos de prueba, ejecución de pruebas funcionales mínimas, cierre de cambio. • Aplicación de las guías de aseguramiento y remediación de vulnerabilidades en ambientes productivos. • Verificación de cumplimiento de las guías de aseguramiento definidas.
Costo aproximado	$ 200.000.000 más IVA
Objetivos de seguridad relacionados	• Proteger, preservar y administrar los activos de información, las bases de datos personales y las tecnologías utilizadas para su procesamiento, frente a amenazas

Av. Calle 26 No. 51- 20, Bogotá, D.C., Colombia
Conmutador: (1) 220 7700 Ext. 1703-1704
fax: 220 7700 Ext. 1283-1269
correo electrónico: contactenos@ins.gov.co
Página web: www.ins.gov.co
Línea gratuita nacional: 018000 113 400

	internas o externas, con el fin de asegurar la confidencialidad, la integridad y disponibilidad, de manera coordinada con las partes involucradas. • Implementar, operar y revisar periódicamente los controles establecidos en la declaración de aplicabilidad, para la prevención y mitigación de los riesgos de seguridad de la información.
Planes de tratamiento de riesgo relacionados	• PT008 • PT010 • PT036 Ver detalle de estos planes en el documento "Plan de tratamiento de riesgos seguridad INS.xlsx entregado por IT Security Services como parte de la consultoría".
Tiempo estimado de ejecución	Anual, permanente

Prioridad	4
Nombre	Servicio SOC o CSIRT para la gestión de incidentes de seguridad y ciberseguridad 7x24
Descripción	Proyecto orientado a lograr un monitoreo permanente y gestión de incidentes de seguridad de la información y ciberseguridad
Alcance	Contratar un servicio de SOC/CSIRT que permita lograr: • Implementación de una solución de análisis y correlación de eventos (SIEM) • Habilitación de la auditoría en los diferentes sistemas de información y dispositivos • Identificación de eventos anómalos de seguridad • Monitoreo de modificación de archivos sensibles • Servicio de caza de amenazas de ciberseguridad o CTH (Cyber Threat Hunting) • Servicio de inteligencia de amenazas de ciberseguridad o CTI (Cyber Threat Intelligence) • Ejecución de simulacros de ocurrencia de incidentes de seguridad y respuesta • Generación de alertas tempranas para riesgos emergentes (vulnerabilidades de día cero, nuevos ataques, nuevas amenazas, entre otros) • Identificación de lecciones aprendidas y oportunidades de mejora
Costo aproximado	$ 312.000.000 más IVA
Objetivos de seguridad relacionados	• Proteger, preservar y administrar los activos de información, las bases de datos personales y las tecnologías utilizadas para su procesamiento, frente a amenazas internas o externas, con el fin de asegurar la confidencialidad, la integridad y disponibilidad, de manera coordinada con las partes involucradas. • Implementar, operar y revisar periódicamente los controles establecidos en la declaración de aplicabilidad, para la prevención y mitigación de los riesgos de seguridad de la información. • Disponer de medidas para atender oportunamente eventos de seguridad de la información con el fin de disminuir los impactos negativos ocasionados por los incidentes de Seguridad de la Información, que se puedan llegar a presentar en la Entidad. • Adopción de Responsabilidad Demostrada con el fin de reducir la probabilidad de violación de la privacidad de los datos personales en de la Entidad. • Fortalecer la cultura de seguridad de la información en la Entidad, a través de la gestión del conocimiento de seguridad de la información.
Planes de tratamiento de riesgo relacionados	• PT004 • PT005

Av. Calle 26 No. 51- 20, Bogotá, D.C., Colombia
Conmutador: (1) 220 7700 Ext. 1703-1704
fax: 220 7700 Ext. 1283-1269
correo electrónico: contactenos@ins.gov.co
Página web: **www.ins.gov.co**
Línea gratuita nacional: 018000 113 400

	• PT037 • PT045 • PT040 • PT050 Ver detalle de estos planes en el documento “Plan de tratamiento de riesgos seguridad INS.xlsx entregado por IT Security Services como parte de la consultoría”.
Tiempo estimado de ejecución	Anual, permanente.

Prioridad	5
Nombre	Plan de continuidad del negocio y redundancias
Descripción	Diseño, implementación y pruebas periódicas a un plan de continuidad de negocio, en el que contemplen instalaciones físicas, procesos de negocio y la plataforma tecnológica del INS
Alcance	Contratar un tercero especializado que permita lograr: • Diagnóstico de cumplimiento del estándar ISO 22301 • Análisis de Impacto al Negocio (BIA) • Análisis de riesgo de continuidad del negocio • Definición de estrategias de recuperación • Desarrollo de planes de continuidad del negocio (BCP) • Desarrollo de planes de recuperación de desastres (DRP) • Acompañamiento en la implementación de los planes • Diseño de plan de pruebas • Acompañamiento en la ejecución de pruebas • Informe de pruebas y oportunidades de mejora
Costo aproximado	$ 245.000.000 más IVA por consultoría más los costos propios de la implementación de BCP y DRP, dependiendo de su diseño.
Objetivos de seguridad relacionados	• Proteger, preservar y administrar los activos de información, las bases de datos personales y las tecnologías utilizadas para su procesamiento, frente a amenazas internas o externas, con el fin de asegurar la confidencialidad, la integridad y disponibilidad, de manera coordinada con las partes involucradas. • Aplicar un proceso de gestión de riesgos de seguridad de la información y bases de datos personales, mediante la ejecución de medidas apropiadas con el fin de identificar, analizar, evaluar, tratar y mitigar los riesgos y así reducir el impacto potencial a niveles aceptables sobre los riesgos asociados con la pérdida de la confidencialidad, de integridad y de disponibilidad. • Disponer de medidas para atender oportunamente eventos de seguridad de la información con el fin de disminuir los impactos negativos ocasionados por los incidentes de Seguridad de la Información, que se puedan llegar a presentar en la Entidad.
Planes de tratamiento de riesgo relacionados	• PT030 • PT046 • PT034 • PT019 • PT035 • PT033 • PT017 Ver detalle de estos planes en el documento “Plan de tratamiento de riesgos seguridad INS.xlsx entregado por IT Security Services como parte de la consultoría”.

Av. Calle 26 No. 51- 20, Bogotá, D.C., Colombia
Conmutador: (1) 220 7700 Ext. 1703-1704
fax: 220 7700 Ext. 1283-1269
correo electrónico: contactenos@ins.gov.co
Página web: www.ins.gov.co
Línea gratuita nacional: 018000 113 400

Tiempo estimado de ejecución	6 meses.

Prioridad	6
Nombre	Fortalecimiento de la seguridad física y ambiental del INS
Descripción	Implementación de controles orientados a mejorar la seguridad física y ambiental (centro de datos), mitigando así los riesgos relacionados.
Alcance	• Acompañamiento a los visitantes por parte del responsable INS • Verificación periódica de las condiciones ambientales de archivos físicos por parte de referentes de proceso, estableciendo planes de acción si es requerido. • Revisión periódica del cableado eléctrico y estructurado, estableciendo planes de acción si es requerido. • Auditoría externa semestral de los controles de seguridad física y análisis de riesgos
Costo aproximado	$ 20.000.000 más IVA por la auditoria externa
Objetivos de seguridad relacionados	• Proteger, preservar y administrar los activos de información, las bases de datos personales y las tecnologías utilizadas para su procesamiento, frente a amenazas internas o externas, con el fin de asegurar la confidencialidad, la integridad y disponibilidad, de manera coordinada con las partes involucradas. • Aplicar un proceso de gestión de riesgos de seguridad de la información y bases de datos personales, mediante la ejecución de medidas apropiadas con el fin de identificar, analizar, evaluar, tratar y mitigar los riesgos y así reducir el impacto potencial a niveles aceptables sobre los riesgos asociados con la pérdida de la confidencialidad, de integridad y de disponibilidad. • Implementar, operar y revisar periódicamente los controles establecidos en la declaración de aplicabilidad, para la prevención y mitigación de los riesgos de seguridad de la información.
Planes de tratamiento de riesgo relacionados	• PT022 • PT031 • PT021 • PT018 Ver detalle de estos planes en el documento “Plan de tratamiento de riesgos seguridad INS.xlsx entregado por IT Security Services como parte de la consultoría”.
Tiempo estimado de ejecución	Anual, periódico.

Prioridad	7
Nombre	Cifrado de portátiles, dispositivos móviles y dispositivos de almacenamiento externo
Descripción	Proteger la información sensible almacenada en portátiles, dispositivos móviles y dispositivos de almacenamiento externo cuando se presente pérdida o robo de los mismos, mediante la implementación de una solución de cifrado.
Alcance	La solución puede ser libre o adquirida, sin embargo, debe contemplar la protección de los siguientes elementos: • Cifrado de portátiles • Cifrado de dispositivos móviles (teléfonos corporativos, PDA, etc.) • Cifrado de dispositivos de almacenamiento (USB, discos duros externos, memorias SD, etc.)
Costo aproximado	Sin costo si se selecciona libre.

Av. Calle 26 No. 51- 20, Bogotá, D.C., Colombia
Conmutador: (1) 220 7700 Ext. 1703-1704
fax: 220 7700 Ext. 1283-1269
correo electrónico: contactenos@ins.gov.co
Página web: www.ins.gov.co
Línea gratuita nacional: 018000 113 400

Objetivos de seguridad relacionados	• Proteger, preservar y administrar los activos de información, las bases de datos personales y las tecnologías utilizadas para su procesamiento, frente a amenazas internas o externas, con el fin de asegurar la confidencialidad, la integridad y disponibilidad, de manera coordinada con las partes involucradas. • Implementar, operar y revisar periódicamente los controles establecidos en la declaración de aplicabilidad, para la prevención y mitigación de los riesgos de seguridad de la información.
Planes de tratamiento de riesgo relacionados	• PT039 Ver detalle de estos planes en el documento “Plan de tratamiento de riesgos seguridad INS.xlsx entregado por IT Security Services como parte de la consultoría”.
Tiempo estimado de ejecución	6 meses

Prioridad	8
Nombre	Implementación de un proceso de desarrollo seguro
Descripción	Garantizar aplicaciones WEB seguras mediante la implementación de un proceso de desarrollo que contemple seguridad a lo largo del ciclo.
Alcance	• Curso de desarrollo y codificación segura para 5 integrantes del área OTIC • Definición de guías de codificación segura • Acompañamiento en la implementación de la metodología de desarrollo seguro y las guías
Costo aproximado	$ 26.000.000 más IVA
Objetivos de seguridad relacionados	• Proteger, preservar y administrar los activos de información, las bases de datos personales y las tecnologías utilizadas para su procesamiento, frente a amenazas internas o externas, con el fin de asegurar la confidencialidad, la integridad y disponibilidad, de manera coordinada con las partes involucradas. • Implementar, operar y revisar periódicamente los controles establecidos en la declaración de aplicabilidad, para la prevención y mitigación de los riesgos de seguridad de la información. • Fortalecer la cultura de seguridad de la información en la Entidad, a través de la gestión del conocimiento de seguridad de la información.
Planes de tratamiento de riesgo relacionados	• PT006 Ver detalle de estos planes en el documento “Plan de tratamiento de riesgos seguridad INS.xlsx entregado por IT Security Services como parte de la consultoría”.
Tiempo estimado de ejecución	3 meses

Prioridad	9
Nombre	Diseño de arquitectura de seguridad informática
Descripción	Proyecto orientado a obtener un diseño de ingeniería que permita fortalecer la seguridad informática del INS
Alcance	Contratar un tercero especialista en diseño de arquitecturas de seguridad informática que permita: • Identificar el estado actual de la arquitectura • Diseñar y planificar las soluciones de seguridad informática necesarias, teniendo en cuenta los análisis de riesgos

Av. Calle 26 No. 51- 20, Bogotá, D.C., Colombia
Conmutador: (1) 220 7700 Ext. 1703-1704
fax: 220 7700 Ext. 1283-1269
correo electrónico: contactenos@ins.gov.co
Página web: **www.ins.gov.co**
Línea gratuita nacional: 018000 113 400

	• Proponer un plan de adquisición e implementación para las soluciones que sea necesario contratar y/o reemplazar, si fuera el caso.
Costo aproximado	$ 20.000.000 más los costos que resulten del diseño de la arquitectura
Objetivos de seguridad relacionados	• Proteger, preservar y administrar los activos de información, las bases de datos personales y las tecnologías utilizadas para su procesamiento, frente a amenazas internas o externas, con el fin de asegurar la confidencialidad, la integridad y disponibilidad, de manera coordinada con las partes involucradas. • Implementar, operar y revisar periódicamente los controles establecidos en la declaración de aplicabilidad, para la prevención y mitigación de los riesgos de seguridad de la información.
Planes de tratamiento de riesgo relacionados	• PT041 Ver detalle de estos planes en el documento “Plan de tratamiento de riesgos seguridad INS.xlsx entregado por IT Security Services como parte de la consultoría”.
Tiempo estimado de ejecución	2 meses.

Prioridad	10
Nombre	Implementación de una solución IDS/IPS
Descripción	Implementación de una solución de detección y prevención de intrusos en las redes del INS.
Alcance	Contratar un tercero para implementar y operar una solución IDS/IPS que permita detectar y/o prevenir intrusiones. La solución debe contar con al menos las siguientes características: • Actualización permanente de firmas • Creación de reglas y excepciones • Integración con SIEM • Generación de alertas • Generación de informes personalizados • Soporte del troughput de INS actual y proyectado
Costo aproximado	$ 60.045.000 más IVA
Objetivos de seguridad relacionados	• Proteger, preservar y administrar los activos de información, las bases de datos personales y las tecnologías utilizadas para su procesamiento, frente a amenazas internas o externas, con el fin de asegurar la confidencialidad, la integridad y disponibilidad, de manera coordinada con las partes involucradas. • Implementar, operar y revisar periódicamente los controles establecidos en la declaración de aplicabilidad, para la prevención y mitigación de los riesgos de seguridad de la información. • Disponer de medidas para atender oportunamente eventos de seguridad de la información con el fin de disminuir los impactos negativos ocasionados por los incidentes de Seguridad de la Información, que se puedan llegar a presentar en la Entidad.
Planes de tratamiento de riesgo relacionados	• PT047 Ver detalle de estos planes en el documento “Plan de tratamiento de riesgos seguridad INS.xlsx entregado por IT Security Services como parte de la consultoría”.
Tiempo estimado de ejecución	Anual, permanente.

Prioridad	11

Av. Calle 26 No. 51- 20, Bogotá, D.C., Colombia
Conmutador: (1) 220 7700 Ext. 1703-1704
fax: 220 7700 Ext. 1283-1269
correo electrónico: contactenos@ins.gov.co
Página web: **www.ins.gov.co**
Línea gratuita nacional: 018000 113 400

Nombre	Borrado y destrucción segura de información
Descripción	Garantizar una eliminación segura de la información digital e impresa, cuando se tiene la certeza de que ya no se necesita.
Alcance	• Adquisición de 20 destructoras de papel • Instalación de una solución de borrado seguro (puede ser libre) que cumpla con el estándar DOD 5220.22
Costo aproximado	$ 4.000.000 más IVA
Objetivos de seguridad relacionados	• Proteger, preservar y administrar los activos de información, las bases de datos personales y las tecnologías utilizadas para su procesamiento, frente a amenazas internas o externas, con el fin de asegurar la confidencialidad, la integridad y disponibilidad, de manera coordinada con las partes involucradas. • Implementar, operar y revisar periódicamente los controles establecidos en la declaración de aplicabilidad, para la prevención y mitigación de los riesgos de seguridad de la información.
Planes de tratamiento de riesgo relacionados	• PT025 • PT024 Ver detalle de estos planes en el documento “Plan de tratamiento de riesgos seguridad INS.xlsx entregado por IT Security Services como parte de la consultoría”.
Tiempo estimado de ejecución	3 meses

Prioridad	12
Nombre	Fortalecimiento de la seguridad de la red
Descripción	Incrementar la seguridad de la red para evitar incidentes de seguridad de la información.

Alcance	• Creación de una lista blanca de las extensiones (por ejemplo PDF, DOCX, XLSX, PPTX, etc.) permitidas para descarga en el INS, garantizando que se bloqueen archivos con extensiones de tipo ejecutables, librerías, imágenes ISO, en el firewall, con el fin de prevenir la descarga de malware en equipos del INS.
	• Cifrado de canales de comunicación o implementación de VPN
	• Contratación de un tercero experto en diseño de redes seguras, permitiendo:
	  ○ Lograr una segmentación de red adecuada
	  ○ Revisar las políticas a nivel de firewall
	  ○ Crear listas de control de acceso
	• Renovación o implementación de los certificados digitales para protección de las comunicaciones de las aplicaciones WEB, considerando la compra de un certificado wildcard (p.ej *.ing.gov.co) que permita proteger todos los subdominios del dominio principal de INS.

Costo aproximado	$ 30.000.000 más IVA de consultoría de red segura más $ 5.000.000 certificado wildcard
Objetivos de seguridad relacionados	• Proteger, preservar y administrar los activos de información, las bases de datos personales y las tecnologías utilizadas para su procesamiento, frente a amenazas internas o externas, con el fin de asegurar la confidencialidad, la integridad y disponibilidad, de manera coordinada con las partes involucradas. • Implementar, operar y revisar periódicamente los controles establecidos en la declaración de aplicabilidad, para la prevención y mitigación de los riesgos de seguridad de la información.
Planes de tratamiento de riesgo relacionados	• PT001 • PT043 • PT041

Av. Calle 26 No. 51- 20, Bogotá, D.C., Colombia
Conmutador: (1) 220 7700 Ext. 1703-1704
fax: 220 7700 Ext. 1283-1269
correo electrónico: contactenos@ins.gov.co
Página web: **www.ins.gov.co**
Línea gratuita nacional: 018000 113 400

	• PT042 Ver detalle de estos planes en el documento “Plan de tratamiento de riesgos seguridad INS.xlsx entregado por IT Security Services como parte de la consultoría”.
Tiempo estimado de ejecución	3 meses

Prioridad	13
Nombre	Seguridad de la información como parte de la arquitectura empresarial
Descripción	Incluir la seguridad de la información en el proyecto de arquitectura empresarial.
Alcance	• Definición de requerimientos de seguridad de la información • Definición de requerimientos de ciberseguridad • Apoyo en actividades de diagnóstico y proyección (AS-IS TO-BE)
Costo aproximado	Directo ninguno, indirecto el tiempo del Oficial de Seguridad para atender la consultoría.
Objetivos de seguridad relacionados	• Proteger, preservar y administrar los activos de información, las bases de datos personales y las tecnologías utilizadas para su procesamiento, frente a amenazas internas o externas, con el fin de asegurar la confidencialidad, la integridad y disponibilidad, de manera coordinada con las partes involucradas. • Adopción de Responsabilidad Demostrada con el fin de reducir la probabilidad de violación de la privacidad de los datos personales en de la Entidad. • Establecer las acciones necesarias, para asegurar la mejora continua del Sistema de Seguridad de la Información y Protección de Datos Personales. • Fortalecer la cultura de seguridad de la información en la Entidad, a través de la gestión del conocimiento de seguridad de la información.
Planes de tratamiento de riesgo relacionados	• PT038 Ver detalle de estos planes en el documento “Plan de tratamiento de riesgos seguridad INS.xlsx entregado por IT Security Services como parte de la consultoría”.
Tiempo estimado de ejecución	Según programación del proyecto de arquitectura empresarial del INS

Prioridad	14
Nombre	Protección de amenazas avanzadas para correo electrónico
Descripción	Incrementar la protección de los buzones de correo electrónico mediante la implementación de una solución de prevención de amenazas avanzadas.
Alcance	La solución debe garantizar protección contra al menos las siguientes amenazas: • APT • Spear Phishing • Ransomware • Scam
Costo aproximado	$ 18.000.000 más IVA
Planes de tratamiento de riesgo relacionados	• PT044

Av. Calle 26 No. 51- 20, Bogotá, D.C., Colombia
Conmutador: (1) 220 7700 Ext. 1703-1704
fax: 220 7700 Ext. 1283-1269
correo electrónico: contactenos@ins.gov.co
Página web: **www.ins.gov.co**
Línea gratuita nacional: 018000 113 400

	Ver detalle de estos planes en el documento “Plan de tratamiento de riesgos seguridad INS.xlsx entregado por IT Security Services como parte de la consultoría”.
Objetivos de seguridad relacionados	• Proteger, preservar y administrar los activos de información, las bases de datos personales y las tecnologías utilizadas para su procesamiento, frente a amenazas internas o externas, con el fin de asegurar la confidencialidad, la integridad y disponibilidad, de manera coordinada con las partes involucradas. • Implementar, operar y revisar periódicamente los controles establecidos en la declaración de aplicabilidad, para la prevención y mitigación de los riesgos de seguridad de la información. • Disponer de medidas para atender oportunamente eventos de seguridad de la información con el fin de disminuir los impactos negativos ocasionados por los incidentes de Seguridad de la Información, que se puedan llegar a presentar en la Entidad.
Tiempo estimado de ejecución	Anual, permanente.

Prioridad	15
Nombre	Implementación de una solución Web Application Firewall (WAF)
Descripción	Incrementar la protección de las aplicaciones WEB del INS antes ataques web bien conocidos, a través de una solución especializada para tal fin.
Alcance	Contratar un tercero para implementar y operar una solución WAF. La solución debe contar con al menos las siguientes características: • Actualización permanente de firmas • Creación de reglas y excepciones • Integración con SIEM • Generación de alertas • Generación de informes personalizados • Soporte del troughput y cantidad de eventos por segundo en la red de INS
Costo aproximado	$ 238.300.000 más IVA
Objetivos de seguridad relacionados	• Proteger, preservar y administrar los activos de información, las bases de datos personales y las tecnologías utilizadas para su procesamiento, frente a amenazas internas o externas, con el fin de asegurar la confidencialidad, la integridad y disponibilidad, de manera coordinada con las partes involucradas. • Implementar, operar y revisar periódicamente los controles establecidos en la declaración de aplicabilidad, para la prevención y mitigación de los riesgos de seguridad de la información. • Disponer de medidas para atender oportunamente eventos de seguridad de la información con el fin de disminuir los impactos negativos ocasionados por los incidentes de Seguridad de la Información, que se puedan llegar a presentar en la Entidad.
Planes de tratamiento de riesgo relacionados	• PT011 Ver detalle de estos planes en el documento “Plan de tratamiento de riesgos seguridad INS.xlsx entregado por IT Security Services como parte de la consultoría”.
Tiempo estimado de ejecución	Anual, permanente.

Prioridad	16

Av. Calle 26 No. 51- 20, Bogotá, D.C., Colombia
Conmutador: (1) 220 7700 Ext. 1703-1704
fax: 220 7700 Ext. 1283-1269
correo electrónico: contactenos@ins.gov.co
Página web: **www.ins.gov.co**
Línea gratuita nacional: 018000 113 400

Nombre	Implementación de una solución Data Base Firewall (DBFW)
Descripción	Incrementar la protección de las bases de datos del INS antes ataques comunes que afectan estas tecnologías, a través de una solución especializada para tal fin.
Alcance	Contratar un tercero para implementar y operar una solución DBFW. La solución debe contar con al menos las siguientes características: • Actualización permanente de firmas • Creación de reglas y excepciones • Integración con SIEM • Generación de alertas • Generación de informes personalizados • Soporte del troughput y cantidad de eventos por segundo en la red de INS
Costo aproximado	$ 303.750.000 más IVA
Objetivos de seguridad relacionados	• Proteger, preservar y administrar los activos de información, las bases de datos personales y las tecnologías utilizadas para su procesamiento, frente a amenazas internas o externas, con el fin de asegurar la confidencialidad, la integridad y disponibilidad, de manera coordinada con las partes involucradas. • Implementar, operar y revisar periódicamente los controles establecidos en la declaración de aplicabilidad, para la prevención y mitigación de los riesgos de seguridad de la información. • Disponer de medidas para atender oportunamente eventos de seguridad de la información con el fin de disminuir los impactos negativos ocasionados por los incidentes de Seguridad de la Información, que se puedan llegar a presentar en la Entidad.
Tiempo estimado de ejecución	Anual, permanente.

Av. Calle 26 No. 51- 20, Bogotá, D.C., Colombia
Conmutador: (1) 220 7700 Ext. 1703-1704
fax: 220 7700 Ext. 1283-1269
correo electrónico: contactenos@ins.gov.co
Página web: **www.ins.gov.co**
Línea gratuita nacional: 018000 113 400

3.2. Programación 2019 - 2021

A continuación, se propone la programación de la ejecución de los proyectos a 3 años:

Proyecto	2019												2020												2021											
	ENE	FEB	MAR	ABR	MAY	JUN	JUL	AGO	SEP	OCT	NOV	DIC	ENE	FEB	MAR	ABR	MAY	JUN	JUL	AGO	SEP	OCT	NOV	DIC	ENE	FEB	MAR	ABR	MAY	JUN	JUL	AGO	SEP	OCT	NOV	DIC
Fase II – Implementación del Sistema de Gestión de Seguridad de la Información																																				
Implementación de Prevención de Fuga de Información (DLP)																																				
Aseguramiento de la plataforma tecnológica y remediación de vulnerabilidades																																				
Servicio SOC o CSIRT para la gestión de incidentes de seguridad y ciberseguridad 7x24																																				
Plan de continuidad del negocio y redundancias																																				
Fortalecimiento de la seguridad física y ambiental del INS																																				
Cifrado de portátiles, dispositivos móviles y dispositivos de almacenamiento externo																																				
Implementación de un proceso de desarrollo seguro																																				
Diseño de arquitectura de seguridad informática																																				
Implementación de una solución IDS/IPS																																				
Borrado y destrucción segura de información																																				
Fortalecimiento de la seguridad de la red																																				
Seguridad de la información como parte de la arquitectura empresarial																																				
Protección de amenazas avanzadas para correo electrónico																																				
Implementación de una solución Web Application Firewall (WAF)																																				
Implementación de una solución Data Base Firewall (DBFW)																																				

Como se ve en la imagen anterior, algunos proyectos se convierten en operación periódica y/o permanente.

3.3. Actualización del PESI

Este plan estratégico se podrá actualizar dependiendo de la ocurrencia de los siguientes hechos:

- Cambios en la estrategia general del INS
- Cambios significativos en la infraestructura tecnológica del INS
- Incidentes de seguridad de la información o ciberseguridad con impacto muy alto

Cabe recordar que las modificaciones al plan deberán ser autorizadas por el Comité de Seguridad de la Información del Instituto.

Av. Calle 26 No. 51- 20, Bogotá, D.C., Colombia
Conmutador: (1) 220 7700 Ext. 1703-1704
fax: 220 7700 Ext. 1283-1269
correo electrónico: contactenos@ins.gov.co
Página web: **www.ins.gov.co**
Línea gratuita nacional: 018000 113 400

BIBLIOGRAFÍA

- DAFP. (2018). Guía para la gestión del riesgo y diseño de controles, en entidades públicas.
- Ministerio de las Tecnologías de Información y Comunicaciones. (1 de abril de 2016). Guía 7 - Guía de gestión de riesgos. Bogotá, Colombia. Obtenido de http://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf

Av. Calle 26 No. 51- 20, Bogotá, D.C., Colombia
Conmutador: (1) 220 7700 Ext. 1703-1704
fax: 220 7700 Ext. 1283-1269
correo electrónico: contactenos@ins.gov.co
Página web: **www.ins.gov.co**
Línea gratuita nacional: 018000 113 400