PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Av. Calle 26 No. 51- 20, Bogotá, D.C., Colombia
Conmutador: (601) 220 77 00 Ext. 1703-1704
correo electrónico: contactenos@ins.gov.co
Página web: **www.ins.gov.co**
Línea gratuita nacional: 018000 113 400

CONTROL DE CAMBIOS

Fecha de actualización	Versión	Creado Por:	Aprobado Por:
28-12-2022	1.0	Joaquín Afanador	

Av. Calle 26 No. 51- 20, Bogotá, D.C., Colombia
Conmutador: (601) 220 77 00 Ext. 1703-1704
correo electrónico: contactenos@ins.gov.co
Página web: www.ins.gov.co
Línea gratuita nacional: 018000 113 400

TABLA DE CONTENIDO

ÍNDICE TABLAS

Av. Calle 26 No. 51- 20, Bogotá, D.C., Colombia
Conmutador: (601) 220 77 00 Ext. 1703-1704
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 el Plan Estratégico de Seguridad y Privacidad de la Información del INS, con el fin de garantizar su operación, monitoreo, revisión y mejora continua.

Esto demuestra que el Instituto Nacional de Salud se encuentra comprometido con la Seguridad de la Información, asignando los recursos necesarios para garantizar que los procesos de la Entidad que se apoyan en la infraestructura tecnológica estén siempre disponibles y protegidos contra cualquier ciberataque, garantizando así, el cumplimiento de sus objetivos estratégicos.

2. OBJETIVO GENERAL

Presentar el Plan Estratégico para operar, monitorear, revisar y mejorar continuamente el Sistema de Gestión de Seguridad de la Información del Instituto Nacional de Salud.

2.1. Objetivos Específicos

- Presentar actividades a desarrollar en los siguientes 2 años, teniendo como base el cumplimiento de los requisitos definidos en la ISO 27001.
- Presentar actividades distribuidas en los niveles estratégico, táctico y operativo.
- Identificar actividades que se deben ejecutar periódicamente (Actividades de Mantenimiento del SGSI).

Av. Calle 26 No. 51- 20, Bogotá, D.C., Colombia
Conmutador: (601) 220 77 00 Ext. 1703-1704
correo electrónico: contactenos@ins.gov.co
Página web: www.ins.gov.co
Línea gratuita nacional: 018000 113 400

3. PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El Plan Estratégico de Seguridad de la Información en el Instituto Nacional de Salud, se desarrollan con base en los resultados del siguiente documento:

- Análisis de Brechas ISO 27001.

Con el fin de entender la estructura de este Plan Estratégico, a continuación se describen los niveles que le componen:

Nivel Estratégico: Plantea actividades a nivel de toma de decisiones de alta dirección y el compromiso de esta instancia, para que el Sistema de Gestión de Seguridad de la Información en el Instituto Nacional de Salud alcance los objetivos propuestos.

Nivel Táctico: Plantea actividades a nivel de toma de decisiones por parte de gerencias o mandos medios, que tienen como fin alcanzar los objetivos del SGSI planteados a nivel estratégico. Se caracteriza por tener actividades a corto plazo, que descomponen las actividades de nivel estratégico en entregables más pequeños.

Nivel Operativo: Describe la operación diaria del SGSI. Traza una hoja de ruta para lograr los objetivos tácticos dentro de un plazo realista. Es detallado y hace énfasis en los objetivos a corto plazo.

A continuación se establecen los responsables, del Plan Estratégico de Seguridad de la Información en el Instituto Nacional de Salud:

- **Comité de Alta Dirección**: La Alta Dirección del Instituto Nacional de Salud, como la máxima autoridad para la toma de decisiones sobre el SGSI.
- **Responsable del Sistema de Seguridad de la Información**: Como responsable de la gestión general del SGSI.
- **Ing. De Seguridad de la Información:** Como el desarrollador de la documentación necesaria para la implementación y operación del SGSI.
- **Oficina de Tecnologías de la Información:** Como ejecutor de los controles tecnológicos.

Av. Calle 26 No. 51- 20, Bogotá, D.C., Colombia
Conmutador: (601) 220 77 00 Ext. 1703-1704
correo electrónico: contactenos@ins.gov.co
Página web: www.ins.gov.co
Línea gratuita nacional: 018000 113 400

A continuación, se describe, a manera general, las actividades que se deben realizar en el año 2023:

Nivel Estratégico	Aprobar los indicadores de gestión del SGSI.	**Nivel Táctico**	Migrar todas las cuentas de correo a Office 365	**Nivel Operativo**	Implementar procedimiento para la Gestión de Incidentes de seguridad de la información.
	Definir el programa de formación, sensibilización y concienciación del SGSI para el año 2023.		Definir acuerdos de niveles de servicio con proveedores (Indicadores de disponibilidad del servicio)		Realizar campaña de etiquetado de activos de información
	Aprobar nueva versión del procedimiento de gestión de incidentes, que incluya el manejo en caso de que se presenten compromisos de datos personales en el INS.		Actualizar el procedimiento de gestión de incidentes, que incluya el manejo en caso de que se presenten compromisos de datos personales en el INS.		Implementar solución DLP para monitorear el uso de información confidencial
	Actividades de mantenimiento		Implementar cláusulas contractuales: * Clausulas de seguridad de la información * Clausulas de continuidad de negocio * Clausulas de propiedad intelectual * Clausulas de confidencialidad * Clausulas de auditoria en seguridad, continuidad y ciberseguridad al proveedor		Llevar a cabo los análisis necesarios para definir el plan de continuidad de negocio y el plan de recuperación de desastres tecnológicos
	Revisar los resultados del SGSI por la Dirección.		Definir el plan de continuidad de negocio y el plan de recuperación de desastres tecnológicos		Poner en funcionamiento o reemplazar el sistema contraincendios del Data Center
	Revisar los resultados de Evaluación de Nivel de Madurez del SGSI.		Definir y llevar a cabo pruebas al plan de continuidad y al DRP		Documentar procedimientos de recuperación de sistemas críticos y de la seguridad informática
	Identificar oportunidades de mejora al SGSI.		***Actividades de mantenimiento***		Revisar periódicamente los derechos de acceso con base en las matrices de roles y perfiles
	Revisión y actualización de políticas, objetivos y métricas del SGSI.		Revisar las políticas específicas y los procedimientos de seguridad de la información con base en las mejores prácticas Anexo A ISO27001 y garantizar su aplicación.		***Actividades de mantenimiento***
	Revisión y actualización de requisitos de las partes interesadas del SGSI.		Medir los indicadores definidos del SGSI.		Actualizar el inventario de activos y contenedores de información.
	Evaluar acciones correctivas originadas en la revisión por la dirección y en las auditorías internas al SGSI		Definir programa de auditorías al SGSI		Actualización del Registro Nacional de Bases de Datos.
	Definir el Portafolio de Proyectos del SGSI para el siguiente año.		Definir matrices de roles y perfiles		Llevar a cabo análisis de riesgos de seguridad de la información con los diferentes procesos del INS
	Garantizar presupuesto del SGSI para el siguiente año.		Dar a conocer las políticas y procedimientos de seguridad de la información al interior del INS.		Realizar campañas de sensibilización y concienciación.
			Aprobar los riesgos residuales de seguridad de la información.		Definir planes de tratamiento para los riesgos residuales de seguridad de la información no tolerables
			Aprobar los planes de tratamiento identificados.		Implementar y monitorear los planes de tratamiento para los riesgos residuales definidos.
			Evaluar el nivel de Madurez del SGSI.		Llevar a cabo análisis vulnerabilidades y hacer seguimiento a la remediación.
					Realizar Auditorías al SGSI.
					Reporte de eventos e incidentes de seguridad de la información.

Tabla 1. Plan Estratégico de Seguridad de la Información – Año 2023

Av. Calle 26 No. 51- 20, Bogotá, D.C., Colombia
Conmutador: (601) 220 77 00 Ext. 1703-1704
correo electrónico: contactenos@ins.gov.co
Página web: **www.ins.gov.co**
Línea gratuita nacional: 018000 113 400

A continuación, se describe, a manera general, las actividades que se deben realizar en el año 2024:

Nivel Estratégico	Plantear la necesidad de certificación de los procesos del INS bajo el estándar ISO 27001.	**Nivel Táctico**	***Actividades de mantenimiento***	**Nivel Operativo**	***Actividades de mantenimiento***
	Actividades de mantenimiento		Revisar las políticas específicas y los procedimientos de seguridad de la información con base en las mejores prácticas Anexo A ISO27001 y garantizar su aplicación.		Actualizar el inventario de activos y contenedores de información.
	Revisar los resultados del SGSI por la Dirección.		Medir los indicadores definidos del SGSI.		Actualización del Registro Nacional de Bases de Datos.
	Revisar los resultados de Evaluación de Nivel de Madurez del SGSI.		Definir programa de auditorías al SGSI		Llevar a cabo análisis de riesgos de seguridad de la información con los diferentes procesos del INS
	Identificar oportunidades de mejora al SGSI.		Dar a conocer las políticas y procedimientos de seguridad de la información al interior del INS.		Realizar campañas de sensibilización y concienciación.
	Revisión y actualización de políticas, objetivos y métricas del SGSI.		Aprobar los riesgos residuales de seguridad de la información.		Definir planes de tratamiento para los riesgos residuales de seguridad de la información no tolerables
	Revisión y actualización de requisitos de las partes interesadas del SGSI.		Aprobar los planes de tratamiento identificados.		Implementar y monitorear los planes de tratamiento para los riesgos residuales definidos.
	Evaluar acciones correctivas originadas en la revisión por la dirección y en las auditorías internas al SGSI		Definir y llevar a cabo pruebas al plan de continuidad y al DRP		Llevar a cabo análisis vulnerabilidades y hacer seguimiento a la remediación.
	Definir el Portafolio de Proyectos del SGSI para el siguiente año.		Evaluar el nivel de Madurez del SGSI.		Realizar Auditorías al SGSI.
	Garantizar presupuesto del SGSI para el siguiente año.				Reporte de eventos e incidentes de seguridad de la información.

Tabla 2. Plan Estratégico de Seguridad de la Información – Año 2024

Av. Calle 26 No. 51- 20, Bogotá, D.C., Colombia
Conmutador: (601) 220 77 00 Ext. 1703-1704
correo electrónico: contactenos@ins.gov.co
Página web: **www.ins.gov.co**
Línea gratuita nacional: 018000 113 400

3.1. Descripción detallada de las actividades a realizar en el Año 2023:

Descripción de Actividades para el Año 2023				
Nivel Estratégico	**Actividad**	**Descripción**	**Responsable**	**Terminación Estimada**
	Aprobar los indicadores de gestión del SGSI.	Aprobar los indicadores de gestión del SGSI para medir la eficacia de los controles o grupos de controles definidos en el Sistema de Gestión de Seguridad de la Información del INS.	Oficina de Tecnologías de la Información	Marzo
	Definir el programa de formación, sensibilización y concienciación del SGSI para el año 2023.	Asegurar que todo el personal del INS y los terceros involucrados, a los que se le asignen responsabilidades definidas en el SGSI esté suficientemente capacitados. Asegurando que todo el personal relevante esté concientizado de la importancia de la seguridad de la información y de cómo contribuye a la consecución de los objetivos del Sistema de Gestión de Seguridad de la Información del INS.	Responsable de Seguridad de la Información	Marzo
	Aprobar nueva versión del procedimiento de gestión de incidentes, que incluya el manejo en caso de que se presenten compromisos de datos personales en el INS.	Aprobar el procedimiento y los mecanismos de gestión de incidentes que permitan una rápida detección y respuesta a los incidentes de seguridad, así como incidentes de protección de datos personales en el INS.	Oficina de Tecnologías de la Información del INS	Marzo

Av. Calle 26 No. 51- 20, Bogotá, D.C., Colombia
Conmutador: (601) 220 77 00 Ext. 1703-1704
correo electrónico: contactenos@ins.gov.co
Página web: **www.ins.gov.co**
Línea gratuita nacional: 018000 113 400

Descripción de Actividades para el Año 2023				
Nivel Estratégico	**Actividad**	**Descripción**	**Responsable**	**Terminación Estimada**
	Actividades de mantenimiento			
	Revisar los resultados del SGSI por la Dirección.	Realizar la Revisión del Sistema de Gestión de Seguridad de la Información del INS por parte del Comité de Seguridad de la Información periódicamente, mínimo semestralmente o cuando ocurran cambios significativos, para garantizar que el alcance definido sigue siendo el adecuado y que las mejoras en el SGSI son evidentes.	Oficina de Tecnologías de la Información	Febrero
	Revisar los resultados de Evaluación de Nivel de Madurez del SGSI.	Realizar la revisión de los Diagnósticos de Sistema de Gestión de Seguridad de la Información del INS, con la finalidad de evaluar si se logró el nivel de madurez propuesto y revisar las estrategias para cumplir las metas definidas.	Oficina de Tecnologías de la Información	Marzo
	Identificar oportunidades de mejora al SGSI.	Identificar e implementar oportunidades de mejora para asegurar que el SGSI alcance los objetivos propuestos.	Oficina de Tecnologías de la Información	Marzo
	Revisión y actualización de políticas, objetivos y métricas del SGSI.	Actualizar objetivos, políticas, procedimientos y métricas del SGSI, en respuesta a cambios internos o externos en los requisitos de negocio, requerimientos de seguridad, procesos de negocio, marco legal, obligaciones contractuales, y riesgos identificados.	Oficina de Tecnologías de la Información	Abril

Av. Calle 26 No. 51- 20, Bogotá, D.C., Colombia
Conmutador: (601) 220 77 00 Ext. 1703-1704
correo electrónico: contactenos@ins.gov.co
Página web: **www.ins.gov.co**
Línea gratuita nacional: 018000 113 400

Descripción de Actividades para el Año 2023				
Nivel Estratégico	**Actividad**	**Descripción**	**Responsable**	**Terminación Estimada**
	Revisión y actualización de requisitos de las partes interesadas del SGSI.	Actualizar y modificar cuando sea necesario los requerimientos de seguridad de las partes interesadas del INS con respecto al marco legal, obligaciones contractuales, niveles de riesgo y criterios de aceptación de riesgos.	Responsable de la Seguridad de la Información	Mayo
	Evaluar acciones correctivas originadas en la revisión por la dirección y en las auditorías internas al SGSI	Evaluar e identificar acciones correctivas adecuadas con base en lecciones aprendidas, las originadas en la revisión por la dirección y las establecidas de acuerdo a las auditorías realizadas a nivel interno las cuales pudieran haber impactado sobre la efectividad o el rendimiento del Sistema de Gestión de Seguridad de la Información del INS.	Oficina de Tecnologías de la Información	Agosto
	Definir el Portafolio de Proyectos del SGSI para el siguiente año.	Proponer y planear los proyectos futuros que fortalezcan la operación y mejora continua del Sistema de Gestión de Seguridad de la Información del INS.	Oficina de Tecnologías de la Información del INS	Noviembre
	Garantizar presupuesto del SGSI para el siguiente año.	Definir y contar con presupuesto adecuado de acuerdo a los proyectos definidos para garantizar la operación y mejora continua del Sistema de Gestión de Seguridad de la Información del INS.	Oficina de Tecnologías de la Información	Diciembre

Tabla 3 Descripción de actividades estratégicas para el año 2023

Av. Calle 26 No. 51- 20, Bogotá, D.C., Colombia
Conmutador: (601) 220 77 00 Ext. 1703-1704
correo electrónico: contactenos@ins.gov.co
Página web: **www.ins.gov.co**
Línea gratuita nacional: 018000 113 400

Descripción de Actividades para el Año 2023				
Nivel Táctico	**Actividad**	**Descripción**	**Responsable**	**Terminación Estimada**
	Migrar todas las cuentas de correo a Office 365	Estudiar la posibilidad de migrar todas las cuentas de correo electrónico al servicio de Office365, priorizando cargos críticos y aquellos en los que se maneja información sensible para la Entidad.	Oficina de Tecnologías de la Información del INS	Abril
	Definir acuerdos de niveles de servicio con proveedores (Indicadores de disponibilidad del servicio)	Definir los acuerdos de nivel de servicio y hacer seguimiento a los mismos garantiza que los servicios contratados con los proveedores operen con normalidad y no se presenten interrupciones	Responsable de la Seguridad de la Información	Abril
	Actualizar el procedimiento de gestión de incidentes, que incluya el manejo en caso de que se presenten compromisos de datos personales en el INS.	Elaborar el procedimiento y los mecanismos de gestión de incidentes que permitan una rápida detección y respuesta a los incidentes de seguridad, así como incidentes de protección de datos personales en el INS.	Ing. De seguridad de la información del INS	Mayo

Av. Calle 26 No. 51- 20, Bogotá, D.C., Colombia
Conmutador: (601) 220 77 00 Ext. 1703-1704
correo electrónico: contactenos@ins.gov.co
Página web: **www.ins.gov.co**
Línea gratuita nacional: 018000 113 400

Descripción de Actividades para el Año 2023				
Nivel Táctico	**Actividad**	**Descripción**	**Responsable**	**Terminación Estimada**
	Implementar cláusulas contractuales: * Clausulas de seguridad de la información * Clausulas de continuidad de negocio * Clausulas de propiedad intelectual * Clausulas de confidencialidad * Clausulas de auditoria en seguridad, continuidad y ciberseguridad al proveedor	Las cláusulas contractuales permite tener mayor control del proveedor, especialmente de aquellos que son proveedores tecnológicos.	Oficina de Tecnologías de la Información del INS	Julio
	Definir el plan de continuidad de negocio y el plan de recuperación de desastres tecnológicos	Documentar el BIA identificando la urgencia de recuperación de cada procedimiento, los recursos y sistemas críticos para estimar el tiempo que el INS puede tolerar en caso de un incidente o desastre, así mismo definiendo los escenarios de desastres a los cuales puede estar expuesto el INS y documentar el plan de continuidad de negocio y el plan de recuperación de desastres.	Ing. De seguridad de la información del INS	Agosto

Av. Calle 26 No. 51- 20, Bogotá, D.C., Colombia
Conmutador: (601) 220 77 00 Ext. 1703-1704
correo electrónico: contactenos@ins.gov.co
Página web: **www.ins.gov.co**
Línea gratuita nacional: 018000 113 400

Descripción de Actividades para el Año 2023				
Nivel Táctico	**Actividad**	**Descripción**	**Responsable**	**Terminación Estimada**
	Definir y llevar a cabo pruebas al plan de continuidad y al DRP	Ejecutar las pruebas definidas en el plan de continuidad de negocio y el plan de recuperación de desastres tecnológicos en el entendido de que ocurra una interrupción que inhabilite las operaciones del INS verificando que los procesos se puedan recuperar a nivel operativo y tecnológico como: datos, hardware y software críticos.	Responsable de Seguridad de la Información	Noviembre
	Actividades de mantenimiento			
	Revisar las políticas específicas y los procedimientos de seguridad de la información con base en las mejores prácticas Anexo A ISO27001 y garantizar su aplicación.	Actualización de los procedimientos y controles que afecten a la seguridad de la información, en respuesta a cambios internos o externos en los requisitos de negocio, requerimientos de seguridad, procesos de negocio, marco legal, obligaciones contractuales, niveles de riesgo y criterios de aceptación de riesgos.	Oficina de Tecnologías de la Información	Febrero
	Medir los indicadores definidos del SGSI.	Medir los indicadores definidos en el SGSI con el fin de monitorear la eficacia de los controles o grupos de controles definidos para el Sistema de Gestión de Seguridad de la Información del INS.	Responsable de Seguridad de la Información	Mayo

Av. Calle 26 No. 51- 20, Bogotá, D.C., Colombia
Conmutador: (601) 220 77 00 Ext. 1703-1704
correo electrónico: contactenos@ins.gov.co
Página web: **www.ins.gov.co**
Línea gratuita nacional: 018000 113 400

Descripción de Actividades para el Año 2023				
Nivel Táctico	**Actividad**	**Descripción**	**Responsable**	**Terminación Estimada**
	Definir programa de auditorías al SGSI	Realizar Programación de Auditorías Internas al Sistema de Gestión de Seguridad de la Información del INS, del año en curso.	Responsable de Seguridad de la Información	Mayo
	Definir matrices de roles y perfiles	Definir matrices de roles y perfiles en las que se observen detalladamente los accesos de la OTIC y de los usuarios más críticos de la Entidad en los diferentes sistemas y servicios tecnológicos.	Responsable de Seguridad de la Información	Junio
	Dar a conocer las políticas y procedimientos de seguridad de la información al interior del INS.	Dar a conocer las políticas de seguridad de la información a todos los interesados del INS y garantizar que las mismas estén implementadas. Esta sensibilización debería realizarse mínimo una vez al año.	Responsable de Seguridad de la Información	Junio
	Aprobar los riesgos residuales de seguridad de la información.	Aprobar los riesgos residuales luego del establecimiento de los controles de los riesgos del INS.	Oficina de Tecnologías de la Información	Junio
	Aprobar los planes de tratamiento identificados.	Aprobar los planes de tratamiento identificados para los riesgos residuales de seguridad de la información.	Oficina de Tecnologías de la Información	Agosto

Av. Calle 26 No. 51- 20, Bogotá, D.C., Colombia
Conmutador: (601) 220 77 00 Ext. 1703-1704
correo electrónico: contactenos@ins.gov.co
Página web: **www.ins.gov.co**
Línea gratuita nacional: 018000 113 400

Descripción de Actividades para el Año 2023				
Nivel Táctico	**Actividad**	**Descripción**	**Responsable**	**Terminación Estimada**
	Evaluar el nivel de Madurez del SGSI.	Realizar el análisis del Instrumento de Identificación de la Línea Base de Seguridad del MSPI Vs los Controles definidos en el Instrumento definido por MINTIC, en cumplimiento a la Estrategia de Gobierno Digital, dando como resultado el Análisis de Madurez de la Seguridad de la Información, que permita identificar planes de acción.	Responsable de la Seguridad de la Información	Diciembre

Tabla 4 Descripción de actividades tácticas para el año 2023

Av. Calle 26 No. 51- 20, Bogotá, D.C., Colombia
Conmutador: (601) 220 77 00 Ext. 1703-1704
correo electrónico: contactenos@ins.gov.co
Página web: **www.ins.gov.co**
Línea gratuita nacional: 018000 113 400

Descripción de Actividades para el Año 2023				
Nivel Operativo	**Actividad**	**Descripción**	**Responsable**	**Terminación Estimada**
	Implementar procedimiento para la Gestión de Incidentes de seguridad de la información.	Implementar el procedimiento y los mecanismos de gestión de incidentes que permitan una rápida detección y respuesta a los incidentes de seguridad, así como incidentes de protección de datos personales en el INS.	Responsable de Seguridad de la Información	Junio
	Realizar campaña de etiquetado de activos de información	Es importante etiquetar la información de acuerdo a los resultados del inventario de activos de información, para facilitar el monitoreo de la información clasificada como confidencial que se encuentre en repositorios electrónicos o físicos no autorizados.	Ing. De seguridad de la información del INS	Agosto
	Implementar solución DLP para monitorear el uso de información confidencial	La implementación de esta solución le permitirá a la Oficina de Tecnologías de la Información del INS, monitorear se la información clasificada como confidencial se encuentra en repositorios electrónicos no autorizados.	Responsable de Seguridad de la Información	Agosto

Av. Calle 26 No. 51- 20, Bogotá, D.C., Colombia
Conmutador: (601) 220 77 00 Ext. 1703-1704
correo electrónico: contactenos@ins.gov.co
Página web: **www.ins.gov.co**
Línea gratuita nacional: 018000 113 400

Descripción de Actividades para el Año 2023				
Nivel Operativo	**Actividad**	**Descripción**	**Responsable**	**Terminación Estimada**
	Llevar a cabo los análisis necesarios para definir el plan de continuidad de negocio y el plan de recuperación de desastres tecnológicos	Documentar el BIA, los escenarios de desastre, el plan de continuidad de negocio y el plan de recuperación de desastres.	Responsable de Seguridad de la Información	Agosto
	Poner en funcionamiento o reemplazar el sistema contraincendios del Data Center	Garantizar el buen funcionamiento del sistema contraincendios del Data Center principal, es una prioridad para la Oficina de Tecnologías de la Información	Oficina de Tecnologías de la Información	Septiembre
	Documentar procedimientos de recuperación de sistemas críticos y de la seguridad informática	Es importante documentar el detalle técnico para recuperar sistemas de información y servicios críticos de la Entidad.	Responsable de Seguridad de la Información	Septiembre
	Revisar periódicamente los derechos de acceso con base en las matrices de roles y perfiles	Se debe revisar periódicamente los derechos de acceso para garantizar que los usuarios tienen permisos de acuerdo a lo autorizado	Ing. De seguridad de la información del INS	Trimestralmente
	Actividades de mantenimiento			
	Actualizar el inventario de activos y contenedores de información.	Mantener actualizado el inventario de activos y riesgos de seguridad de la información y su correspondiente valoración.	Ing. De seguridad de la información del INS	Mayo

Av. Calle 26 No. 51- 20, Bogotá, D.C., Colombia
Conmutador: (601) 220 77 00 Ext. 1703-1704
correo electrónico: contactenos@ins.gov.co
Página web: **www.ins.gov.co**
Línea gratuita nacional: 018000 113 400

Descripción de Actividades para el Año 2023				
Nivel Operativo	**Actividad**	**Descripción**	**Responsable**	**Terminación Estimada**
	Actualización del Registro Nacional de Bases de Datos.	Actualizar el Registro Nacional de Base de Datos ante la Superintendencia de Industria y Comercio de las Bases de Datos Personales identificadas en el Servicio Geológico Colombiano.	Ing. De seguridad de la información del INS	Mayo
	Llevar a cabo análisis de riesgos de seguridad de la información con los diferentes procesos del INS	Realizar la identificación de los activos de información y Datos Personales, que están dentro del alcance del Sistema de Gestión de Seguridad de la Información. Así como evaluar los riesgos de seguridad de la información que afecten la confidencialidad, integridad o disponibilidad de la información.	Ing. De seguridad de la información del INS	Mayo

Av. Calle 26 No. 51- 20, Bogotá, D.C., Colombia
Conmutador: (601) 220 77 00 Ext. 1703-1704
correo electrónico: contactenos@ins.gov.co
Página web: **www.ins.gov.co**
Línea gratuita nacional: 018000 113 400

Descripción de Actividades para el Año 2023				
Nivel Operativo	**Actividad**	**Descripción**	**Responsable**	**Terminación Estimada**
	Realizar campañas de sensibilización y concienciación.	Dar capacitaciones y concientizar a todo el personal del INS y los terceros involucrados, a los que se le asignen responsabilidades definidas en el SGSI y verificar que estén suficientemente capacitados. Asegurando que todo el personal esté concientizado de la importancia de la seguridad de la información y de cómo contribuye a la consecución de los objetivos del Sistema de Gestión de Seguridad de la Información del INS.	Responsable de la Seguridad de la Información	Mayo
	Definir planes de tratamiento para los riesgos residuales de seguridad de la información no tolerables	Plantear y ejecutar planes de tratamiento que identifiquen las acciones, los recursos, las responsabilidades y las prioridades para gestionar los riesgos residuales no tolerables de seguridad de la información.	Ing. De seguridad de la información del INS	Julio
	Implementar y monitorear los planes de tratamiento para los riesgos residuales definidos.	Ejecutar y hacer seguimiento a las acciones identificadas, los recursos, las responsabilidades y las prioridades para gestionar los riesgos de seguridad de la información.	Responsable de Seguridad de la Información	Agosto

Av. Calle 26 No. 51- 20, Bogotá, D.C., Colombia
Conmutador: (601) 220 77 00 Ext. 1703-1704
correo electrónico: contactenos@ins.gov.co
Página web: **www.ins.gov.co**
Línea gratuita nacional: 018000 113 400

Descripción de Actividades para el Año 2023				
Nivel Operativo	**Actividad**	**Descripción**	**Responsable**	**Terminación Estimada**
	Llevar a cabo análisis vulnerabilidades y hacer seguimiento a la remediación.	Realizar la planeación y ejecución de Análisis de Vulnerabilidades a los sistemas de información y servicios tecnológicos críticos de la Entidad de manera periódica.	Ing. De seguridad de la información del INS	Septiembre
	Realizar Auditorías al SGSI.	Llevar a cabo auditorías al Sistema de Gestión de Seguridad de la Información del INS, para identificar oportunidades de mejora.	Responsable de Seguridad de la Información	Septiembre
	Reporte de eventos e incidentes de seguridad de la información.	Identificar brechas, detectar y prevenir eventos e incidentes de seguridad de la información.	Responsable de la Seguridad de la Información	Mensual

Tabla 5 Descripción de actividades operativo para el año 2023

Av. Calle 26 No. 51- 20, Bogotá, D.C., Colombia
Conmutador: (601) 220 77 00 Ext. 1703-1704
correo electrónico: contactenos@ins.gov.co
Página web: **www.ins.gov.co**
Línea gratuita nacional: 018000 113 400

3.2. Descripción detallada de las actividades a realizar en el Año 2024:

Descripción de Actividades para el Año 2024				
Nivel Estratégico	**Actividad**	**Descripción**	**Responsable**	**Terminación Estimada**
	Plantear la necesidad de certificación de los procesos del INS bajo el estándar ISO 27001.	La Oficina de Tecnologías de la Información puede plantear que se lleve a cabo un proceso de certificación bajo el estándar ISO 27001, según los resultados del nivel de madurez del SGSI.	Responsable de Seguridad de la Información	Noviembre
	Actividades de mantenimiento			
	Revisar los resultados del SGSI por la Dirección.	Realizar la Revisión del Sistema de Gestión de Seguridad de la Información del INS por parte del Comité de Seguridad de la Información periódicamente, mínimo semestralmente o cuando ocurran cambios significativos, para garantizar que el alcance definido sigue siendo el adecuado y que las mejoras en el SGSI son evidentes.	Oficina de Tecnologías de la Información	Febrero

Av. Calle 26 No. 51- 20, Bogotá, D.C., Colombia
Conmutador: (601) 220 77 00 Ext. 1703-1704
correo electrónico: contactenos@ins.gov.co
Página web: **www.ins.gov.co**
Línea gratuita nacional: 018000 113 400

Descripción de Actividades para el Año 2024				
Nivel Estratégico	**Actividad**	**Descripción**	**Responsable**	**Terminación Estimada**
	Revisar los resultados de Evaluación de Nivel de Madurez del SGSI.	Realizar la revisión de los Diagnósticos de Sistema de Gestión de Seguridad de la Información del INS, con la finalidad de evaluar si se logró el nivel de madurez propuesto y revisar las estrategias para cumplir las metas definidas	Oficina de Tecnologías de la Información	Marzo
	Identificar oportunidades de mejora al SGSI.	Identificar e implementar oportunidades de mejora para asegurar que el SGSI alcance los objetivos propuestos.	Oficina de Tecnologías de la Información	Marzo
	Revisión y actualización de políticas, objetivos y métricas del SGSI.	Actualizar objetivos, políticas, procedimientos y métricas del SGSI, en respuesta a cambios internos o externos en los requisitos de negocio, requerimientos de seguridad, procesos de negocio, marco legal, obligaciones contractuales, y riesgos identificados.	Oficina de Tecnologías de la Información	Abril
	Revisión y actualización de requisitos de las partes interesadas del SGSI.	Actualizar y modificar cuando sea necesario los requerimientos de seguridad de las partes interesadas del INS con respecto al marco legal, obligaciones contractuales, niveles de riesgo y criterios de aceptación de riesgos.	Responsable de la Seguridad de la Información	Mayo

Av. Calle 26 No. 51- 20, Bogotá, D.C., Colombia
Conmutador: (601) 220 77 00 Ext. 1703-1704
correo electrónico: contactenos@ins.gov.co
Página web: **www.ins.gov.co**
Línea gratuita nacional: 018000 113 400

Descripción de Actividades para el Año 2024				
Nivel Estratégico	**Actividad**	**Descripción**	**Responsable**	**Terminación Estimada**
	Evaluar acciones correctivas originadas en la revisión por la dirección y en las auditorías internas al SGSI	Evaluar e identificar acciones correctivas adecuadas con base en lecciones aprendidas, las originadas en la revisión por la dirección y las establecidas de acuerdo a las auditorías realizadas a nivel interno las cuales pudieran haber impactado sobre la efectividad o el rendimiento del Sistema de Gestión de Seguridad de la Información del INS.	Oficina de Tecnologías de la Información	Agosto
	Definir el Portafolio de Proyectos del SGSI para el siguiente año.	Proponer y planear los proyectos futuros que fortalezcan la implementación y operación del Sistema de Gestión de Seguridad de la Información del INS.	Oficina de Tecnologías de la Información del INS	Noviembre
	Garantizar presupuesto del SGSI para el siguiente año.	Definir y contar con presupuesto adecuado de acuerdo a los proyectos definidos para garantizar la operación y mejora continua del Sistema de Gestión de Seguridad de la Información del INS.	Oficina de Tecnologías de la Información	Diciembre

Tabla 6 Descripción de actividades estratégicas para el año 2024

Av. Calle 26 No. 51- 20, Bogotá, D.C., Colombia
Conmutador: (601) 220 77 00 Ext. 1703-1704
correo electrónico: contactenos@ins.gov.co
Página web: **www.ins.gov.co**
Línea gratuita nacional: 018000 113 400

Descripción de Actividades para el Año 2024				
Nivel Táctico	**Actividad**	**Descripción**	**Responsable**	**Terminación Estimada**
	Actividades de mantenimiento			
	Revisar las políticas específicas y los procedimientos de seguridad de la información con base en las mejores prácticas Anexo A ISO27001 y garantizar su aplicación.	Actualización de los procedimientos y controles que afecten a la seguridad de la información, en respuesta a cambios internos o externos en los requisitos de negocio, requerimientos de seguridad, procesos de negocio, marco legal, obligaciones contractuales, niveles de riesgo y criterios de aceptación de riesgos.	Oficina de Tecnologías de la Información	Febrero
	Medir los indicadores definidos del SGSI.	Medir los indicadores definidos en el SGSI con el fin de monitorear la eficacia de los controles o grupos de controles definidos para el Sistema de Gestión de Seguridad de la Información del INS.	Responsable de Seguridad de la Información	Mayo
	Definir programa de auditorías al SGSI	Realizar Programación de Auditorías Internas al Sistema de Gestión de Seguridad de la Información del INS, del año en curso.	Responsable de Seguridad de la Información	Mayo
	Dar a conocer las políticas y procedimientos de seguridad de la información al interior del INS.	Dar a conocer las políticas de seguridad de la información a todos los interesados del INS y garantizar que las mismas estén implementadas. Esta sensibilización debería realizarse mínimo una vez al año.	Responsable de Seguridad de la Información	Junio

Av. Calle 26 No. 51- 20, Bogotá, D.C., Colombia
Conmutador: (601) 220 77 00 Ext. 1703-1704
correo electrónico: contactenos@ins.gov.co
Página web: **www.ins.gov.co**
Línea gratuita nacional: 018000 113 400

Descripción de Actividades para el Año 2024				
Nivel Táctico	**Actividad**	**Descripción**	**Responsable**	**Terminación Estimada**
	Aprobar los riesgos residuales de seguridad de la información.	Aprobar los riesgos residuales luego del establecimiento de los controles de los riesgos del INS.	Oficina de Tecnologías de la Información	Junio
	Aprobar los planes de tratamiento identificados.	Aprobar los planes de tratamiento identificados para los riesgos residuales de seguridad de la información.	Oficina de Tecnologías de la Información	Agosto
	Definir y llevar a cabo pruebas al plan de continuidad y al DRP	Ejecutar las pruebas definidas en el plan de continuidad de negocio y el plan de recuperación de desastres tecnológicos en el entendido de que ocurra una interrupción que inhabilite las operaciones del INS verificando que los procesos se puedan recuperar a nivel operativo y tecnológico como: datos, hardware y software críticos.	Responsable de Seguridad de la Información	Noviembre
	Evaluar el nivel de Madurez del SGSI.	Realizar el análisis del Instrumento de Identificación de la Línea Base de Seguridad del MSPI Vs los Controles definidos en el Instrumento definido por MINTIC, en cumplimiento a la Estrategia de Gobierno Digital, dando como resultado el Análisis de Madurez de la Seguridad de la Información, que permita identificar planes de acción.	Responsable de la Seguridad de la Información	Diciembre

Tabla 7 Descripción de actividades tácticas para el año 2024

Av. Calle 26 No. 51- 20, Bogotá, D.C., Colombia
Conmutador: (601) 220 77 00 Ext. 1703-1704
correo electrónico: contactenos@ins.gov.co
Página web: **www.ins.gov.co**
Línea gratuita nacional: 018000 113 400

Descripción de Actividades para el Año 2024				
Nivel Operativo	**Actividad**	**Descripción**	**Responsable**	**Terminación Estimada**
	Actividades de mantenimiento			
	Actualizar el inventario de activos y contenedores de información.	Mantener actualizado el inventario de activos y riesgos de seguridad de la información y su correspondiente valoración.	Ing. De seguridad de la información del INS	Mayo
	Actualización del Registro Nacional de Bases de Datos.	Actualizar el Registro Nacional de Base de Datos ante la Superintendencia de Industria y Comercio de las Bases de Datos Personales identificadas en el Servicio Geológico Colombiano.	Ing. De seguridad de la información del INS	Mayo
	Llevar a cabo análisis de riesgos de seguridad de la información con los diferentes procesos del INS	Realizar la identificación de los activos de información y Datos Personales, que están dentro del alcance del Sistema de Gestión de Seguridad de la Información. Así como evaluar los riesgos de seguridad de la información que afecten la confidencialidad, integridad o disponibilidad de la información.	Ing. De seguridad de la información del INS	Mayo

Av. Calle 26 No. 51- 20, Bogotá, D.C., Colombia
Conmutador: (601) 220 77 00 Ext. 1703-1704
correo electrónico: contactenos@ins.gov.co
Página web: **www.ins.gov.co**
Línea gratuita nacional: 018000 113 400

Descripción de Actividades para el Año 2024				
Nivel Operativo	**Actividad**	**Descripción**	**Responsable**	**Terminación Estimada**
	Realizar campañas de sensibilización y concienciación.	Dar capacitaciones y concientizar a todo el personal del INS y los terceros involucrados, a los que se le asignen responsabilidades definidas en el SGSI y verificar que estén suficientemente capacitados. Asegurando que todo el personal esté concientizado de la importancia de la seguridad de la información y de cómo contribuye a la consecución de los objetivos del Sistema de Gestión de Seguridad de la Información del INS.	Responsable de la Seguridad de la Información	Mayo
	Definir planes de tratamiento para los riesgos residuales de seguridad de la información no tolerables	Plantear y ejecutar planes de tratamiento que identifiquen las acciones, los recursos, las responsabilidades y las prioridades para gestionar los riesgos residuales no tolerables de seguridad de la información.	Ing. De seguridad de la información del INS	Julio
	Implementar y monitorear los planes de tratamiento para los riesgos residuales definidos.	Ejecutar y hacer seguimiento a las acciones identificadas, los recursos, las responsabilidades y las prioridades para gestionar los riesgos de seguridad de la información.	Responsable de Seguridad de la Información	Agosto
	Llevar a cabo análisis vulnerabilidades y hacer seguimiento a la remediación.	Realizar la planeación y ejecución de Análisis de Vulnerabilidades a los sistemas de información y servicios tecnológicos críticos de la Entidad de manera periódica.	Ing. De seguridad de la información del INS	Septiembre

Av. Calle 26 No. 51- 20, Bogotá, D.C., Colombia
Conmutador: (601) 220 77 00 Ext. 1703-1704
correo electrónico: contactenos@ins.gov.co
Página web: **www.ins.gov.co**
Línea gratuita nacional: 018000 113 400

Descripción de Actividades para el Año 2024				
Nivel Operativo	**Actividad**	**Descripción**	**Responsable**	**Terminación Estimada**
	Realizar Auditorías al SGSI.	Llevar a cabo auditorías al Sistema de Gestión de Seguridad de la Información del INS, para identificar oportunidades de mejora.	Responsable de la Seguridad de la Información	Septiembre
	Reporte de eventos e incidentes de seguridad de la información.	Identificar brechas, detectar y prevenir eventos e incidentes de seguridad de la información.	Responsable de la Seguridad de la Información	Mensual

Tabla 8 Descripción de actividades operativo para el año 2024

Av. Calle 26 No. 51- 20, Bogotá, D.C., Colombia
Conmutador: (601) 220 77 00 Ext. 1703-1704
correo electrónico: contactenos@ins.gov.co
Página web: **www.ins.gov.co**
Línea gratuita nacional: 018000 113 400

BIBLIOGRAFÍA

- Norma ISO 27001:2013: Tecnología De La Información. Técnicas De Seguridad. Sistemas De Gestión De La Seguridad De La Información (SGSI). Requisitos.
- Norma ISO/IEC 27032:2012 .Tecnologías de la información - Técnicas de seguridad - Directrices para la Ciberseguridad.

Av. Calle 26 No. 51- 20, Bogotá, D.C., Colombia
Conmutador: (601) 220 77 00 Ext. 1703-1704
correo electrónico: contactenos@ins.gov.co
Página web: **www.ins.gov.co**
Línea gratuita nacional: 018000 113 400

GLOSARIO

Activo de información: *Sustenta uno o más procesos de negocio. En otras palabras, es todo aquello que tiene valor para la organización.*

Análisis de riesgo: *Elemento de control que permite establecer la probabilidad de ocurrencia de los eventos positivos y/o negativos y el impacto de sus consecuencias calificándolas y evaluándolos a fin de determinar la capacidad de la Entidad para su aceptación y manejo.*

Acceso a la Información *Pública Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados.*

Activo *En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).*

Activo de Información *Cualquier componente (sea humano, tecnológico, software, etc.) que sustenta uno o más procesos de negocios de una unidad o área de negocio. En otras palabras, es todo aquello que tiene valor para la organización. En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.*

Auditoría *Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y obviamente para determinar el grado en el que se cumplen los criterios de auditoría.*

La Autenticidad*, esta propiedad permite asegurar el origen de la información. La identidad del emisor puede ser validada, de modo que se puede demostrar que es quien dice ser.*

BIA: *Business Impact Analysis (Análisis de Impacto al Negocio): El proceso de análisis de las funciones de negocio y el efecto que una interrupción del negocio podría tener sobre ellos.*

Ciberseguridad: *Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).*

Ciberespacio*: Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009)*

Confidencialidad: *Propiedad que determina que la información no está disponible ni sea revelada a individuos, Entidades o procesos no autorizados.*

Continuidad del Negocio: *Describe los procesos y procedimientos que una organización pone en marcha para garantizar que las funciones esenciales puedan continuar durante y después de un desastre.*

Contenedor: *Cualquier componente (sea humano, tecnológico, software, etc.) que contenga uno o más activos de información.*

Av. Calle 26 No. 51- 20, Bogotá, D.C., Colombia
Conmutador: (601) 220 77 00 Ext. 1703-1704
correo electrónico: contactenos@ins.gov.co
Página web: **www.ins.gov.co**
Línea gratuita nacional: 018000 113 400

Disponibilidad: *Propiedad de que la información sea accesible y utilizable por solicitud de una Entidad autorizada.*

Evento de seguridad de la información *Presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad.*

Gestión de incidentes de seguridad de la información *Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).*

Gestión del riesgo: *La gestión del riesgo se refiere a los principios y metodología para la gestión eficaz del riesgo, mientras que gestionar el riesgo se refiere a la aplicación de estos principios y metodología a riesgos particulares.*

Incidente de seguridad de la información*: Un evento o serie de eventos de seguridad de la información no deseados o inesperados que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.*

Integridad: *Propiedad de salvaguardar la exactitud y estado completo de los activos.*

MTPD: *(Maximum Tolerable Period of Disruption) Periodo Máximo Tolerable de interrupción.*

Partes interesadas (Stakeholder) *Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.*

Plan de Continuidad del Negocio: *(o sus siglas en inglés **BCP**, por Business Continuity Plan) es un plan logístico de cómo una organización debe recuperar y restaurar sus funciones críticas parcialmente o totalmente interrumpidas dentro de un tiempo predeterminado después de una interrupción no deseada o desastre.*

Plan de Recuperación de Desastres (DRP): *Conjunto de procedimientos y estrategias definidos para asegurar la reanudación oportuna y ordenada de los servicios informáticos.*

Plan de tratamiento de riesgos *Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).*

Privacidad: *En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL la correlativa obligación de proteger dicha información en observancia del marco legal vigente.*

Registro Nacional de Bases de Datos: *Directorio público de las bases de datos sujetas a Tratamiento que operan en el país. (Ley 1581 de 2012, art 25)*

Riesgo residual: *Nivel restante del riesgo después del tratamiento del riesgo.*

Av. Calle 26 No. 51- 20, Bogotá, D.C., Colombia
Conmutador: (601) 220 77 00 Ext. 1703-1704
correo electrónico: contactenos@ins.gov.co
Página web: **www.ins.gov.co**
Línea gratuita nacional: 018000 113 400

Seguridad de la Información *Preservación de la confidencialidad, la integridad y la disponibilidad de la información; además puede involucrar otras propiedades tales como, autenticidad, trazabilidad, no repudio y fiabilidad.*

Sistema de Gestión de Seguridad de la Información *Parte del sistema de gestión global, basado en un enfoque hacia los riesgos globales de un negocio, cuyo fin es establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la Seguridad de la Información.*

Tratamiento del riesgo: *Proceso de selección e implementación de medidas para modificar el riesgo.*

Vulnerabilidad*: Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).*

Av. Calle 26 No. 51- 20, Bogotá, D.C., Colombia
Conmutador: (601) 220 77 00 Ext. 1703-1704
correo electrónico: contactenos@ins.gov.co
Página web: **www.ins.gov.co**
Línea gratuita nacional: 018000 113 400