MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO GEOGRÁFICO NACIONAL	Código: SGSI-MA-01 Versión: 1.0	

Elaborado:	Revisado por:	Aprobado por:
Oficina de Estadística e Informática	Gerencia General Oficina de Asesoría Jurídica	Jefatura

INDICE

Contenido

1. OBJETIVO

Este presente manual tiene como objetivo definir, implementar, mantener y mejorar continuamente un marco de gestión adecuado para preservar la confidencialidad, integridad y disponibilidad de la información del Instituto Geográfico Nacional, teniendo en cuenta el alcance, los requisitos de seguridad de la información, los riesgos identificados y controles de seguridad de la información aplicables de acuerdo al alcance establecido según la a Norma NTP ISO/IEC 27001:2014.

2. ALCANCE

La presente Política de Seguridad de la Información es de aplicación:

- A todo el personal del Instituto Geográfico Nacional, sin distinción del régimen laboral, contractual o nivel jerárquico.
- A todo el personal natural o jurídico que presta servicios en general o que tengan acceso a la información de propiedad del Instituto Geográfico Nacional.

3. BASE LEGAL

3.1. Decreto Supremo N.º 029-2021-PCM que aprueba el Reglamento del Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital y establece disposiciones sobre las condiciones, requisitos y uso de las tecnologías y medios electrónicos en el procedimiento administrativo.
3.2. Resolución ministerial 004-2016-PCM. Se aprueba el uso obligatorio de la Norma Técnica Peruana “NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2ª Edición”, en todas las entidades integrantes del Sistema Nacional de Informática.
3.3. Ley N° 29733, Ley de Protección de Datos Personales.
3.4. Ley del Instituto Geográfico Nacional, Ley Nº 27292, publicada el 27 de junio del año 2000.
3.5. Resolución Jefatural N.° 0106-2014/IGN/OAJ. Se aprueba El Código de Ética del Instituto Geográfico Nacional.

1. TÉRMINOS Y DEFINICIONES

1.1. Seguridad de la Información: Todas las acciones orientadas a preservar la integridad, confidencialidad y disponibilidad de la información y los activos asociados a su tratamiento independiente de la forma en la que la información se encuentre.

1.2. Activo de información: Cualquier información que tiene valor para la Entidad y para el Sistema de Gestión de Seguridad de la Información. Se consideran también los recursos humanos, tecnológicos que intervienen en el tratamiento directo o indirecto de la información, así como sus procesos y actividades.

1.3. Análisis de riesgo: Proceso de comprender la naturaleza del riesgo y determinar el nivel de riesgo.

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

1.5. Confidencialidad: Propiedad de la información que hace que no esté disponible o que sea revelada a individuos o entidades no autorizados.

1.6. Disponibilidad: Propiedad de ser accesible y utilizable ante la demanda de una entidad autorizada.

1.7. Gestión de Riesgo: Aplicación sistemática de políticas de gestión procedimientos y prácticas a las actividades de comunicación, consulta, establecimiento del contexto e identificación, análisis, evaluación, tratamiento, seguimiento y revisión de riesgos.

1.8. Sistema de gestión de seguridad de la información: Es un componente del sistema de gestión de una organización, basado en un enfoque de riesgos, que tiene como función establecer, implementar, operar, supervisar, revisar, mantener y mejorar la seguridad de la información.

1.9. Personal: Se refiere a todo el personal del Instituto Geográfico Nacional, sin distinción del régimen laboral, contractual o nivel jerárquico, personal natural o jurídico que presta servicios en general o que tengan acceso a la información geoespacial de propiedad del Instituto Geográfico.

2. CONTEXTO DE LA ORGANIZACIÓN

2.1. Creación

El 23 de junio del 2000, se promulga la Ley del Instituto Geográfico Nacional (Ley N° 27292), incluyendo su organización y funciones.

2.2. Misión

Elaborar y actualizar la Cartografía Básica Oficial del Perú, proporcionando a las entidades públicas y privadas la cartografía que requieran para los fines del desarrollo y la Defensa Nacional.

2.3. Visión

Ser una entidad estratégica rectora y líder en la generación, administración y validación de datos geoespaciales de calidad, con tecnología de última generación, que satisfaga la demanda de la información geoespacial confiable para la sociedad de usuarios en el ámbito nacional.

2.4. Comprensión de las necesidades y expectativas de las partes interesadas

Se identifica en función al análisis del contexto externo e interno de la Institución, así como sus necesidades respecto a la seguridad de la información de las partes interesadas.

Contexto Externo

El Instituto Geográfico Nacional tiene que cumplir con los requisitos regulatorio y normativos como:

- Implementación de la Norma Técnica Peruana “NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a. Edición”.
- Implementación de la Ley de Protección de Datos Personales (Ley N° 29733) y su Reglamento (Decreto Supremo N° 003-2013-JUS), los cuales están muy vinculados a aspectos de seguridad de la información.
- Cumplir con la normatividad informática según lo definido por la Secretaría de Gobierno Digital de la PCM.

Contexto Interno

- El Instituto Geográfico Nacional requiere también capacitar y sensibilizar al personal en temas de seguridad de la información, lo que permitirá el cumplimiento de los controles de seguridad.
- El Instituto Geográfico Nacional ha identificado la necesidad de implementar un Sistema de Gestión de Seguridad de la Información para mejorar la seguridad de la información.

Teniendo claro el contexto externo e interno podemos identificar y Comprender las Necesidades y Expectativas de las Partes Interesadas

- La Presidencia del Consejo de Ministros (PCM), espera el cumplimiento de la implementación del SGSI, de acuerdo a lo solicitado por la Secretaría de Gobierno Digital (SeGDi).
- La Autoridad Nacional de Protección de Datos Personales del Ministerio de Justicia y Derechos Humanos, debe registrar el cumplimiento de la Ley de Protección de Datos Personales.
- La Jefatura, requiere el cumplimiento de los objetivos y requisitos del SGSI.
- El Personal del Instituto Geográfico Nacional, necesita ser concientizado y capacitado en temas de Seguridad de la Información.

2.5. Determinar el alcance del Sistema de Gestión de Seguridad de la Información

Considerando el análisis del contexto externo e interno, así como las partes interesadas y sus respectivas necesidades, El Instituto Geográfico Nacional define el alcance del SGSI, en la Gestión de Operaciones de la sala de servidores, ubicado en la sede principal en la Avenida Andrés Aramburú 1184, Surquillo.

3. LIDERAZGO Y COMPROMISO DEL SGSI.

3.1. Liderazgo y compromiso

El Instituto Geográfico Nacional, demuestra su liderazgo y compromiso con el Sistema de Gestión de Seguridad de la Información (SGSI) con las siguientes acciones:

- Se han establecido lineamientos de seguridad de la información, los cuales se encuentran alineados a los objetivos del Instituto Geográfico Nacional.
- Asegurando la disponibilidad de recursos necesarios para el SGSI.
- Comunicando la importancia de una gestión eficaz de la seguridad de la información.
- Dirigiendo y apoyando al personal para contribuir a la eficacia del SGSI.
- Promoviendo la mejora continua del SGSI.

3.2. Política

El Instituto Geográfico Nacional cuenta con una política de seguridad de la información el cual establece como objetivo: “Proteger la información del Instituto Geográfico Nacional - IGN y la infraestructura tecnológica utilizada para su procesamiento, frente a amenazas internas / externas, deliberadas / accidentales, con el fin de asegurar la confidencialidad, integridad y disponibilidad de la información.”

3.3. Funciones Organizacionales, Responsabilidades y Autoridades en la organización

Los roles y responsabilidades de seguridad de la información priorizan la protección de activos de información sobre la base de los pilares de seguridad de la información.

a. Alta Dirección del IGN

Representada por el Jefe del IGN, tiene la responsabilidad y autoridad para:

- Designar mediante Resolución Jefatural al Comité de Gobierno Digital.
- Designar mediante Resolución Jefatural al Oficial de seguridad de la información.

b. Comité de Gobierno Digital del IGN

El Comité de Gobierno Digital del IGN tendrá las siguientes responsabilidades:

- Gestionar la asignación de personal y recursos necesarios para la implementación del SGSI.
- Elaborar informes anuales que evalúen el desempeño del SGSI.

c. Oficial de Seguridad de la Información

Tendrán las siguientes responsabilidades:

- Asegurar el funcionamiento SGSI conforme a la NTP ISO/IEC 27001:2014.
- Mantener actualizado los documentos generados en el marco del SGSI.
- Asistir al personal de la entidad y a las personas que presten servicios, cualquiera sea su condición o modalidad contractual en materia de seguridad de la información.
- Coordinar con las Secretaría de Gobierno Digital de la Presidencia de Consejo de Ministros el cumplimiento de las disposiciones en materia de seguridad de la información.
- Revisar los riesgos de seguridad de la información de la entidad y coordinar la elaboración de los planes de tratamiento, en coordinación con los responsables
- Identificar las actividades de difusión y sensibilización en seguridad de la información.
- Elaborar y evaluar informes del cumplimiento del SGSI.

d. Oficina de Estadística e Informática

Tendrán las siguientes responsabilidades:

- Establecer, mantener y documentar el sistema de seguridad de la información en el marco de la normativa vigente.
- Administrar los procesos de seguridad de la información.
- Proponer las directrices necesarias para la implementación de las soluciones tecnológicas en la entidad.
- Identificar, gestionar y actualizar los riesgos e incidentes de seguridad de la información en el IGN, asegurando su tratamiento oportuno, en coordinación con el Oficial de Seguridad de la información.

e. Oficina de Abastecimiento

Tendrán las siguientes responsabilidades:

- Incluir en los contratos con proveedores de bienes o servicios, cuya actividad pueda afectar directa o indirectamente a la seguridad de la información de la entidad, cláusulas referidas a la confidencialidad e integridad.

- Incluir el contrato de quienes prestan servicios bajo la modalidad de locador el cumplimiento de la “Política de Seguridad de la Información” aprobado con Resolución Jefatural N° 051-2022/IGN/GG/OEINFO, el 09 de marzo del 2022” y “Directiva Lineamientos de seguridad para lograr niveles de protección y control de la información digital”, aprobado con Resolución Jefatural N° 097-2022/IGN/GG/OEINFO el 06 de junio del 2022.

f. Oficina de Recursos Humanos

Tendrán las siguientes responsabilidades:

- Asegurar que el personal que se contrata cumpla con el perfil profesional que se requiere para el puesto de trabajo.
- Hacer de conocimiento e Incluir en el contrato del personal que labora en el IGN, el cumplimiento de la “Política de Seguridad de la Información” aprobado con Resolución Jefatural N° 051-2022/IGN/GG/OEINFO, el 09 de marzo del 2022” y “Directiva Lineamientos de seguridad para lograr niveles de protección y control de la información digital”, aprobado con Resolución Jefatural N° 097-2022/IGN/GG/OEINFO el 06 de junio del 2022.

g. Los Directores, Sub Directores y Jefes

Tendrán las siguientes responsabilidades:

- Brindar las facilidades correspondientes para la implementación y actualización del SGSI.
- Apoyar en el cumplimiento de los documentos y controles de SGSI para el personal a su cargo.
- Brindar las facilidades al personal a su cargo y a las personas que presten servicios, cualquier sea su condición o modalidad contractual para que participen en los eventos de sensibilización y/o capacitación.

h. Personal del IGN

Tendrán las siguientes responsabilidades:

- Cumplir con las disposiciones señaladas en los documentos y controles generados en el marco del SGSI.
- Utilizar la información del Instituto Geográfico Nacional únicamente para los propósitos autorizados.

- Participar en las actividades de capacitación y sensibilización en temas de seguridad de la información.
- Reportar al Oficial de Seguridad el incumplimiento de las disposiciones señaladas en los documentos y controles generados en el marco del SGSI.
- Reportar cualquier brecha o vulnerabilidad de seguridad de la información en los sistemas utilizados al Oficial de Seguridad.
- Reportar al Oficial de Seguridad de la información y/o a los responsables de las Direcciones, Sub Direcciones, Oficias y/o procesos posibles no conformidades, observaciones u oportunidades de mejora.

3.4. Política

El Instituto Geográfico Nacional, cuenta con una Política de Seguridad de la Información el cual establece: “Proteger la información del Instituto Geográfico Nacional - IGN y la infraestructura tecnológica utilizada para su procesamiento, frente a amenazas internas / externas, deliberadas / accidentales, con el fin de asegurar la confidencialidad, integridad y disponibilidad de la información” y efectuar el mejoramiento continuo del Sistema de Gestión de Seguridad de la Información (SGSI).

4. PLANIFICACION DEL SGSI

4.1. Acciones para abordar los riesgos y Oportunidades

Para determinar los riesgos de seguridad de la información y oportunidades del SGSI se deberá considerar lo señalado en los numerales 2.2, 2.3, 2.4 y 2.5 del presente manual.
Los riesgos y oportunidades se determinan con la finalidad de:

- Asegurar que el SGSI logre los resultados esperados.
- Prevenir o reducir efectos indeseados.
- Lograr la mejora continua.

El Oficial de Seguridad de la información y los responsables de los órganos y/o procesos, en el marco de la metodología de gestión de riesgos vigente, aplicarán la metodología indicada en el numeral n. Gestión de Riesgos, de la DIRECTIVA N°016-2022/GG/OEINFO, “Lineamientos de seguridad para lograr niveles de protección y control de la información digital en el Instituto Geográfico Nacional”.

4.2. Objetivos del Sistema de Gestión de Seguridad de la información

El Instituto Geográfico Nacional define los siguientes objetivos del Sistema de Gestión de Seguridad de la información:

- Implementar el Sistema de Gestión de Seguridad de la Información para preservar la confidencialidad, integridad y disponibilidad en el IGN.
- Cumplir con la implementación de la Norma NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a. Edición".
- Desarrollar un programa de difusión, sensibilización y capacitación en base al Sistema de Gestión de Seguridad de la Información para el personal involucrado, el cual permitirá un mejor conocimiento y participación de las actividades que forman parte del mismo.
- Implementar las métricas e indicadores del Sistema de Gestión de Seguridad de la Información.

5. GESTIÓN DEL SOPORTE Y OPERACIÓN DEL SGSI

5.1. Gestión de recursos

Los recursos para la implementación del Sistema de Gestión de Seguridad de la Información, serán gestionados a través del Comité de Gobierno Digital, de acuerdo las funciones asignadas.

5.2. Competencia

El personal cuenta con las competencias necesarias para desarrollar sus funciones, así como también reciben información en materia de seguridad de la información.

5.3. Concientización

Uno de los elementos básicos para el éxito de un SGSI es el recurso humano, por tal motivo para lograr la concientización del personal involucrado en el SGSI, se realizan charlas, capacitaciones y/o talleres de sensibilización en temas de seguridad de la información. Su eficacia se realizará mediante una evaluación presencial, virtual o mediante una auditoría interna al menos una vez al año, con el fin de verificar la comprensión del personal del IGN.

El Oficial de Seguridad de la Información conservará el registro de las evaluaciones realizadas.

Los resultados obtenidos podrán ser empleados como referencia para la determinación de futuros programas de sensibilización. Este proceso es gestionado por la Oficina de Recursos Humanos en coordinación con el Oficial de Seguridad de la Información.

5.4. Gestión de la comunicación

El Instituto Geográfico Nacional determina que las comunicaciones internas y externas, relacionadas al SGSI deben realizarse de la siguiente manera.

Comunicaciones Internas, cuentan con los siguientes canales de comunicación:

- Reuniones presenciales o virtuales.
- Sistema de Trámite Documentario para documentos internos (INTRADOC)
- Intranet del IGN.
- Inducciones, capacitaciones y talleres presenciales o virtuales.
- Correo institucional.

Comunicaciones Externas, cuentan con los siguientes canales de comunicación:

- Sistema de Trámite Documentario (SISTRADOC)
- Página web institucional.
- Correo electrónico.
- Mesa de partes.
- Redes sociales.

El Oficial de Seguridad de la Información en coordinación con el Comité de Gobierno Digital, son los responsables de comunicar a los terceros de la información pertinente respecto al SGSI o sobre incidentes que ocurran.

5.5. Gestión de información documentada

a) Creación y Actualización

Para la creación y actualización de documentos relacionados al SGSI deben contar con la siguiente información:

- Título del documento.
- Elaborado por
- Revisado por
- Aprobado por
- Código del documento
- Versión del documento.
- Fecha de aprobación del documento.

El código del documento se compone de la siguiente manera: SGSI-**XX**-V.**X**, donde el valor que cambia es donde están las **XX**, que son las dos primeras letras del documento formulado. Ejemplo, si fuera un manual seria SGSI-**MA**-V.**1.** En el caso que dos tipos de documentos tengan igual las dos primeras letras se toman las tres primeras letras.

La aprobación de los documentos se realiza de acuerdo a la siguiente tabla N° 01.

Tabla N° 01: Control y aprobación de documentos.

Tipo de documento	Aprobación del documento
Política, Directivas, Manuales	Jefe del IGN
Procedimientos, Instrucciones, Formularios, Check List, Guías, Formatos, Catálogos, registros y similares.	El jefe de la OEINFO, con VB. del Gerente General.

- Para la gestión de los documentos relacionados al SGSI, se aplicará la siguiente jerarquía de documentos.

b) Control de la Información Documentada

Para el control de la información documentada referente al SGSI, la organización debe abordar las siguientes actividades:

- La distribución o acceso de la información documentada será de forma física o digital utilizando los diferentes medios señalados en el numeral 5.4 del presente manual.
- El almacenamiento y preservación de la documentación, es responsabilidad de la OEINFO, quien tomará las medidas y controles necesarios para almacenar y proteger la documentación.

- Los niveles de control y autorizaciones de la información documentada se detallan en la siguiente tabla N° 02

Tabla N° 02: Control de documentos

Clasificar por Tipo de información documentada	Responsable de controlarlo	Forma de controlar el documento
Política, Manuales, Directivas	El administrativo de OEINFO, es el responsable de controlar la información documentada	Lista Maestra de Información Documentada Interna
Procedimientos, Guías, Formatos, Catálogos, etc.	El administrativo de OEINFO, es el responsable de controlar la información documentada	Lista Maestra de Información Documentada Interna

- La Lista Maestra de información documentada interna se encuentra detallada en el anexo N° 01, permite tener el control de los documentos, y los cambios de versión. Se muestra el formato de la Lista Maestra.

5.6. Gestión de riesgos de seguridad de la información

El IGN, ha definido una Metodología de Gestión de Riesgos, el cual contiene las fases de Preparación, Valoración (Inventario de activos, Análisis de riesgo, Evaluación de riesgo) y Tratamiento del riesgo se encuentra en el numeral “n” de la Directiva N°016-2022-IGN-OEINFO, “Lineamientos de seguridad para lograr niveles de protección y control de la información digital en el Instituto Geográfico Nacional”.

La declaración de aplicabilidad es un documento basado en el anexo A de la norma ISO 27001:2013 que agrupa 114 controles en 14 dominios. A través de la declaración de aplicabilidad el Instituto Geográfico Nacional identifica los controles aplicables que serán implementados como parte del SGSI, ver anexo N° 02.

6. EVALUACIÓN DE DESEMPEÑO DEL SGSI

6.1. Indicadores y métricas

Los responsables de las Oficinas, Direcciones y Sub Direcciones y/o procesos, en coordinación con el Oficial de Seguridad de la información, determinarán los controles de seguridad de la información que requerirán medición periódica, los cuales serán registrados por el Oficial de Seguridad

de la información en el Anexo N° 03, denominado Monitoreo de controles de seguridad de información; asimismo, registrará los resultados de la medición de los objetivos del SGSI en el Anexo N° 04, denominado Seguimiento de los objetivos del SGSI.

6.2. Auditoria internas

Al menos una vez al año se realizará una auditoría interna en el Instituto Geográfico Nacional, de acuerdo con el Anexo N° 05, Pautas para la auditoría interna del SGSI, con el objetivo de verificar que el SGSI se encuentre conforme a lo dispuesto en la normatividad de la materia.

6.3. Revisión del SGSI

El Oficial de Seguridad presentará un informe sobre el SGSI al Comité de Gobierno Digital, al menos una vez al año con la finalidad de asegurar su conveniencia, adecuación y eficacia continua. Todo ello será documentado como parte de la implementación del SGSI.

El informe debe incluir los siguientes puntos:

a. Cambios que podrían afectar al SGSI
b. Retroalimentación sobre el desempeño del SGSI, relativas a:
    - No conformidades y acciones correctivas.
    - Resultados de seguimiento y mediciones.
    - Resultados de auditorías.
    - Cumplimiento de los objetivos del SGSI.
c. La retroalimentación de las partes interesadas.
d. Los resultados de la evaluación de riesgos de seguridad de la información.
e. Las oportunidades de mejora del SGSI.

ANEXOS

ANEXOS N° 01: Lista Maestra de información documentada del SGSI

N°	CODIGO	TÍTULO DEL DOCUMENTO	VERSION	RESPONSABLE DE ELABORACION	DOCUMENTO DE APROBACION	FECHA DE APROBACION

ANEXOS N° 02: Declaración de Aplicabilidad

CLAUSULA		OBJETIVOS DE CONTROL			CONTROL	APLICA (SI/NO)	MOTIVO DE APLICABILIDAD	EVIDENCIA
A5	Políticas de seguridad de la información	5.1	Directrices de gestión para la seguridad de la información.	5.1.1	Políticas para la seguridad de la información			
				5.1.2	Revisión de las políticas para la seguridad de la información			
A6	Organización de la seguridad de la información	6.1	Organización interna.	6.1.1	Roles y responsabilidades para la seguridad de la información			
				6.1.2	Segregación de funciones			
				6.1.3	Contacto con las autoridades			
				6.1.4	Contacto con grupos de interés especial.			
				6.1.5	Seguridad de la información en la gestión de proyectos			
		6.2	Dispositivos móviles y teletrabajo.	6.2.1	Política de dispositivos móviles.			
				6.2.2	Teletrabajo			
A7	Seguridad ligada a los Recursos Humanos	7.1	Antes de la contratación.	7.1.1	Selección.			
				7.1.2	Términos y condiciones de contratación			
		7.2	Durante la contratación	7.2.1	Responsabilidades de gerencia.			
				7.2.2	Concientización, educación y capacitación en seguridad de la información.			
				7.2.3	Proceso disciplinario.			
		7.3	Cese o cambio de puesto de trabajo	7.3.1	Cese o cambio de responsabilidades del trabajo.			
A8	Gestión de activos	8.1	Responsabilidad sobre los activos	8.1.1	Inventario de activos			
				8.1.2	Propiedad de los activos			
				8.1.3	Uso aceptable de los activos			
				8.1.4	Retorno de activos.			
		8.2	Clasificación de la información	8.2.1	Clasificación de la información			
				8.2.2	Etiquetado de la información.			
				8.2.3	Manejo de activos			
		8.3	Manejo de los medios	8.3.1	Gestión de medios removibles			
				8.3.2	Disposición de medios			
				8.3.3	Transferencia de medios físicos			

A9	Control de accesos	9.1	Requisitos de negocio	9.1.1	Política de control de accesos			
				9.1.2	Acceso a redes y servicios			
		9.2	Gestión de acceso de usuario.	9.2.1	Registro y baja de usuarios			
				9.2.2	Aprovisionamiento de acceso a usuario			
				9.2.3	Gestión de los derechos de acceso privilegiado			
				9.2.4	Gestión de información de autentificación secreta de usuarios.			
				9.2.5	Revisión de los derechos de acceso de los usuarios.			
				9.2.6	Remoción o ajuste de los derechos de acceso			
		9.3	Responsabilidades de los usuarios	9.3.1	Uso de información de autentificación secreta			
		9.4	Control de acceso a sistema y aplicación.	9.4.1	Restricción del acceso a la información.			
				9.4.2	Procedimientos de ingreso seguro			
				9.4.3	Sistema de gestión de contraseñas			
				9.4.4	Uso de programas utilitarios privilegiados.			
				9.4.5	Control de acceso al código fuente de los programas			
A10	Cifrado	10.1	Controles criptográficos	10.1.1	Política de uso de los controles criptográficos.			
				10.1.2	Gestión de claves			
A11	Seguridad física y ambiental	11.1	Áreas seguras	11.1.1	Perímetro de seguridad física			
				11.1.2	Control de ingreso físico.			
				11.1.3	Asegurar oficinas, áreas e instalaciones			
				11.1.4	Protección contra las amenazas externas y ambientales.			
				11.1.5	Trabajo en áreas seguras.			
				11.1.6	Áreas de despacho y carga			
		11.2	Equipos	11.2.1	Emplazamiento y protección de equipos			
				11.2.2	Servicios de suministro.			
				11.2.3	Seguridad del cableado.			
				11.2.4	Mantenimiento de equipos.			
				11.2.5	Remoción de activos			
				11.2.6	Seguridad de los equipos y activos fuera de las instalaciones.			
				11.2.7	Disposición o reutilización segura de equipos			
				11.2.8	Equipo informático de usuario desatendido.			
				11.2.9	Política de escritorio limpio y pantalla limpia			

A12	Seguridad de las operaciones	12.1	Procedimiento y responsabilidades operativas	12.1.1	Documentación de procedimientos de operación			
				12.1.2	Gestión de cambios			
				12.1.3	Gestión de capacidades.			
				12.1.4	Separación de entornos de desarrollo, prueba y operaciones.			
		12.2	Protección contra código malicioso	12.2.1	Controles contra el código malicioso			
		12.3	Respaldo	12.3.1	Respaldo de información			
		12.4	Registros y monitoreo	12.4.1	Registro de eventos (logs)			
				12.4.2	Protección de información de registros			
				12.4.3	Registros de administrador y operador			
				12.4.4	Sincronización de reloj			
		12.5	Control del software en explotación	12.5.1	Instalación de software en sistemas operacionales			
		12.6	Gestión de la vulnerabilidad	12.6.1	Gestión de vulnerabilidades técnicas.			
				12.6.2	Restricción sobre la instalación de software			
		12.7	Consideraciones de las auditorías de los sistemas de información	12.7.1	Controles de auditoría de sistemas de información.			
A13	Seguridad en las comunicaciones	13.1	Gestión de la seguridad en las redes	13.1.1	Controles de red			
				13.1.2	Mecanismos de seguridad asociados a servicios en red.			
				13.1.3	Segregación de redes			
		13.2	Intercambio de información con partes externas.	13.2.1	Políticas y procedimientos de intercambio de información.			
				13.2.2	Acuerdos de intercambio.			
				13.2.3	Mensajería electrónica.			
				13.2.4	Acuerdos de confidencialidad y secreto			
A14	Adquisición, desarrollo y mantenimiento de los sistemas de información	14.1	Requisitos de seguridad de los sistemas de información.	14.1.1	Análisis y especificación de los requisitos de seguridad.			
				14.1.2	Aseguramiento de servicios de aplicaciones sobre redes públicas			
				14.1.3	Protección de las transacciones por redes telemáticas.			
		14.2	Seguridad en los procesos de desarrollo y soporte.	14.2.1	Política de desarrollo seguro de software.			
				14.2.2	Procedimientos de control de cambios del sistema			
				14.2.3	Revisión técnica de aplicaciones después de cambios a la plataforma operativa.			
				14.2.4	Restricciones sobre cambios a los paquetes de software			
				14.2.5	Principios de ingeniería de sistemas seguros.			
				14.2.6	Ambiente de desarrollo seguro			
				14.2.7	Desarrollo contratado externamente.			
				14.2.8	Pruebas de seguridad del sistema.			
				14.2.9	Pruebas de aceptación del sistema			
		14.3	Datos de prueba	14.3.1	Protección de los datos de pruebas			

A15	Relaciones con proveedores	15.1	Seguridad de la información en las relaciones con proveedores	15.1.1	Política de seguridad de la información para proveedores			
				15.1.2	Tratamiento del riesgo dentro de acuerdos de proveedores.			
				15.1.3	Cadena de suministro en tecnologías de la información y comunicaciones.			
		15.2	Gestión de la prestación del servicio por proveedores.	15.2.1	Supervisión y revisión de los servicios prestados por terceros.			
				15.2.2	Gestión de cambios en los servicios prestados por terceros			
A16	Gestión de incidentes en la seguridad de la información	16.1	Gestión de incidentes de seguridad de la información y mejoras.	16.1.1	Responsabilidades y procedimientos.			
				16.1.2	Reporte de eventos de seguridad de la información			
				16.1.3	Reporte de debilidades de seguridad de la información.			
				16.1.4	Evaluación y decisión sobre eventos de seguridad de la información			
				16.1.5	Respuesta a los incidentes de seguridad de la información.			
				16.1.6	Aprendizaje de los incidentes de seguridad de la información			
				16.1.7	Recolección de evidencias.			
A17	Aspectos de seguridad de la información en la gestión de la continuidad del negocio	17.1	Continuidad de la seguridad de la información.	17.1.1	Planificación de la continuidad de la seguridad de la información.			
				17.1.2	Implementación de continuidad de seguridad de la información.			
				17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información			
		17.2	Redundancias	17.2.1	Disponibilidad de instalaciones para el procesamiento de la información			
A18	Cumplimiento	18.1	Cumplimiento con los requisitos legales y contractuales.	18.1.1	Identificación de requisitos contractuales y de legislación aplicable			
				18.1.2	Derechos de propiedad intelectual			
				18.1.3	Protección de registros			
				18.1.4	Privacidad y protección de datos personales			
				18.1.5	Regulación de controles criptográficos.			
		18.2	Revisiones de la seguridad de la información	18.2.1	Revisión independiente de seguridad de la información			
				18.2.2	Cumplimiento de políticas y normas de seguridad.			
				18.2.3	Revisión de cumplimiento técnico.			

ANEXOS N° 03: Monitoreo de controles de seguridad de información

CONTROL DE SEGURIDAD DE LA INFORMACIÓN	INDICADOR	OBJETIVO	RESPONSABLE	Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Set	Oct	Nov	Dic

ANEXOS N° 04: Seguimiento de los Controles del SGSI

CONTROL DE SEGURIDAD DE LA INFORMACIÓN	INDICADOR	OBJETIVO	RESPONSABLE	VARIABLES	METODO DE CALCULO	LOGRO DE OBTENIDO

ANEXO 5: PAUTAS PARA LA AUDITORÍA INTERNA DEL SGSI

1. OBJETIVO

Establecer las pautas para la planificación y ejecución de las auditorías internas del SGSI en el Instituto Geográfico Nacional.

2. DESARROLLO

2.1. Generalidades.

a. El proceso de auditoría interna del SGSI, constará de las siguientes etapas:
   - Programación de la auditoría interna.
   - Selección de auditores internos.
   - Planificación de la auditoría interna.
   - Desarrollo de la auditoría interna.
   - Resultados de la auditoría interna.

b. La participación del personal del IGN en el proceso de la auditoría interna del SGSI deberá ser colaborativa, íntegra y transparente.

c. El Oficial de Seguridad deberá acompañar a los responsables de las Direcciones, Sub Direcciones, Oficinas y/o procesos durante el desarrollo de la auditoría interna, así como proporcionar soporte cuando se requiera.

d. Se dispondrá las acciones respectivas, en base a los resultados obtenidos en la auditoría interna, con el objetivo de garantizar la mejora continua del SGSI del Instituto Geográfico Nacional.

2.2. Proceso de auditoría interna.

2.2.1. Programación de la auditoría interna

Durante el primer trimestre de cada año, el Oficial de Seguridad de la información, programará las auditorías internas, a través del formato 1 Programa anual de auditorías internas, tomando en cuenta lo siguiente:

- Según su importancia
- Según los resultados de auditorías previas.
- Según la disponibilidad de recursos.

Durante la programación de las auditorías internas se priorizará lo siguiente:

- Los que presentan No conformidades en auditorías anteriores.
- Aquellos procesos priorizados por la Alta Dirección o el Comité de Gobierno Digital

2.2.2. Selección de auditores

El Oficial de Seguridad de la información deberá seleccionar a los miembros del equipo auditor, el cual estará conformado por:

- Un auditor líder
- Un auditor

Requisitos mínimos para cada miembro del equipo auditor

a. Auditor líder:

- **Personal de la entidad:**
  - Título profesional.
  - Haber laborado al menos seis (6) meses en la entidad.
  - Contar con formación de auditor interno en la ISO NTP/IEC 27001:2014.

- **Personal externo:**
  - Título profesional.
  - Contar con conocimientos en la ISO NTP/IEC 27001:2014.
  - Haber participado previamente en auditorías internas en sistemas de gestión de seguridad de la información.

b. Auditor:

- **Personal de la entidad:**
  - Haber laborado al menos tres (3) meses en la entidad.
  - Contar con formación de auditor interno en la ISO NTP/IEC 27001:2014.

- **Personal externo:**
  - Título profesional o bachiller
  - Contar con conocimientos en la ISO NTP/IEC 27001:2014.

– Haber participado previamente en auditorías internas en sistemas de gestión de seguridad de la información.

2.2.3. Planificación de la auditoría interna.

Previo a la auditoría interna programada, el auditor líder coordinará con los auditados, las acciones para el desarrollo de la auditoría interna registrando las mismas en el Formato 2: Plan de auditoría interna. Asimismo, dicho Plan de auditoría deberá ser comunicado a los auditados.

2.2.4. Desarrollo de auditoría interna.

a. Solicitud de documentos

Previo a la auditoría interna, el auditor líder, mediante solicitud expresa, solicitará al Oficial de Seguridad de la información documentación referida al SGSI.

b. Reunión de apertura

La reunión de apertura será liderado por el auditor líder y participarán los responsables de las Direcciones, Sub Direcciones, Oficinas y/o procesos auditados y el equipo auditor. Durante la reunión de apertura, mínimamente se desarrollará lo siguiente:

- Presentación del equipo auditor.
- Objetivos de la auditoría.
- Alcance de la auditoría.
- Confidencialidad de la información levantada.
- Ajustes al Plan de Auditoría, de ser el caso.

c. Ejecución de auditoría interna

La auditoría interna estará basada en la recopilación de evidencia objetiva sobre el grado de cumplimiento de los requisitos de la ISO NTP/IEC 27001:2014 y los controles comprendidos en su Anexo A: Objetivos de control y controles de referencia, para lo cual se realizarán las siguientes actividades:

- Revisión de la información documentada.
- Entrevistas al personal involucrado dentro del alcance del SGSI.

- Recorrido de las instalaciones para verificación de controles físicos de seguridad de la información.
- Revisión de la gestión de riesgos de seguridad de la información y oportunidades de mejora en el SGSI

Como resultado de estas actividades, el equipo auditor identificará hallazgos que evidencien el cumplimiento de los requisitos de la ISO NTP/IEC 27001:2014 y los controles comprendidos en el precitado Anexo A.

d. Reunión de cierre

Culminada la auditoría interna, se efectuará la reunión de cierre, en la cual el auditor líder informará a los responsables de las Direcciones, Sub Direcciones, Oficinas y/o procesos respecto a:

- El resumen de actividades desarrolladas.
- Los hallazgos encontrados durante su ejecución.
- Las fortalezas del SGSI de la entidad.
- La fecha de entrega del informe de auditoría interna

2.2.5. Resultados de la auditoría interna.

El auditor líder, en coordinación con el equipo auditor, elaborará el informe de auditoría interna, conforme al formato 3 Informe de auditoría interna. Los resultados deberán ser coherentes con lo informado en la reunión de cierre.

El informe de auditoría interna será remitido al Oficial de Seguridad de la información, dentro de los diez (10) días hábiles de concluida la auditoría, quien comunicará o difundirá el informe a los responsables de las Direcciones, Sub Direcciones, Oficinas y/o procesos auditados, a fin que ejecuten y/o implementen las recomendaciones, observaciones u oportunidades de mejora, de corresponder.

3. FORMATO

Formato 1: Programa anual de auditorías internas.
Formato 2: Plan de auditoría interna.
Formato 3: Informe de auditoría interna.

Formato 1: Programa anual de auditorías internas

ALCANCE	RESPONSABLE DE AUDITAR (LIDER AUDITOR Y AUDITOR)	AÑO											
		Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Set	Oct	Nov	Dic

Formato 2: Plan de auditoria interna

1. PLAN DE AUDITORIA INTERNA	
FECHA PROGRAMADA	
AUDITOR LIDER	
AUDITOR/ES	

ALCANCE	FECHA	HORA	RESPONSABLE

Formato 3: Informe de la auditoria interna

1. Datos de la auditoria	
ALCANCE	
AUDITOR LIDER	
AUDITOR/ES	
FECHAS DE LA AUDITORIA	
FECHA DE EMISION DEL INFORME	

Objetivo de la auditoria
No Conformidades
Observaciones
Oportunidades de Mejora
Conclusiones