IX. ANEXOS

Anexo I

Determinación del Alcance del Sistema de Gestión de la Seguridad de la Información

De acuerdo con la NTP ISO/IEC 27001:2014, se consideraron los aspectos internos y externos referidos en la cláusula 4.1 (comprender la organización y su contexto), los requisitos referidos en la cláusula 4.2 (comprender las necesidades y expectativas de las partes interesadas) y las interfaces y dependencias entre actividades realizadas por la organización y las que son efectuadas por otras organizaciones. Tras ello, se determinó que el Instituto Geofísico del Perú ha interiorizado los requisitos de la norma NTP ISO/IEC 27001:2014 para el siguiente alcance:

Generación de la Información Sísmica Nacional

Este alcance tiene como límite físico las siguientes sedes del IGP:

- Calle Badajoz, 169; Urb. Mayorazgo - IV Etapa; Ate, Lima
- Calle Calatrava N° 216 , Urb. Camino Real, La Molina, Lima
- Estaciones de la Red Sísmica Nacional que brindan datos en tiempo real

En función a procesos, el alcance abarca los siguientes procesos y sus activos de información:

- Planificación y dirección
- Sistema de Gestión
- Comunicaciones
- Operaciones y Mantenimiento
- Procesamiento de Información Sísmica
- Gestión del Sistema de Recursos Humanos
- Gestión de Logística y Servicios Generales
- Gestión de Tecnología de la Información

En función de unidades orgánicas, abarca:

- Oficina de Tecnología de la Información y Datos Geofísicos
- Oficina de Planeamiento y Presupuesto
- Subdirección de Ciencias de la Tierra Sólida
- Subdirección de Redes Geofísicas
- Unidad de Logística
- Unidad de Recursos Humanos
- Unidad Funcional de Comunicaciones

Anexo II

Objetivos de la Seguridad de la Información

- Proteger la confidencialidad de la información asegurando que sea accesible a entidades o personas debidamente autorizadas.
- Salvaguardar la integridad de la información para garantizar su exactitud y totalidad, así como sus métodos de procesamiento.
- Asegurar la disponibilidad de la información sísmica y los sistemas de información que soportan el proceso de su generación, para las entidades y personas autorizadas de acuerdo con los estándares y acuerdos establecidos.
- Establecer, implementar, mantener y mejorar el sistema de gestión de seguridad de la información del IGP

Anexo III

Roles y Responsabilidades Generales del Sistema de Gestión de la Seguridad de la Información

1. Comité de Gobierno Digital

Conformado por:

- El Gerente General, en representación del titular de la Entidad.
- El Director Científico, como líder del gobierno digital.
- La Jefa de la Oficina de Tecnologías de la Información y Datos Geofísicos.
- El Jefe de la Unidad de Recursos Humanos.
- El Responsable del área de atención al ciudadano.
- El Oficial de Seguridad de la Información.
- El Jefe de la Oficina de Asesoría Jurídica.
- El Jefe de la Oficina de Planeamiento y Presupuesto.

Tiene como funciones:

a) Formular el Plan de gobierno Digital en coordinación con los órganos, unidades orgánicas, programas y/o proyectos de la entidad.
b) Liderar y dirigir el proceso de transformación digital en la entidad.
c) Evaluar que el uso actual y futuro de las tecnologías digitales sea acorde con los cambios tecnológicos, regulatorios, necesidades de la entidad, objetivos institucionales, entre otros, con miras a implementar el Gobierno Digital.
d) Gestionar la asignación de personal y recursos necesarios para la implementación del Plan de gobierno Digital, Modelo de Gestión Documental (MGD), Modelo de Datos Abiertos Gubernamentales y Sistema de Gestión de Seguridad de la Información (SGSI) en sus Planes Operativos Institucionales, Plan Anual de contrataciones y otros.
e) Promover y gestionar la implementación de estándares y buenas prácticas en gestión y gobierno de tecnologías digitales, interoperabilidad, seguridad digital, identidad digital y datos en la entidad.
f) Elaborar informes anuales que midan el progreso de la implementación del Plan de Gobierno Digital y evalúen el desempeño del Modelo de Gestión Documental (MGD), Modelo de Datos abiertos Gubernamentales y Sistema de Gestión de Seguridad de la Información (SGSI).
g) Vigilar el cumplimiento de la normatividad relacionada con la implementación del gobierno digital, interoperabilidad, seguridad de la información y datos abiertos en las entidades púbicas.
h) Promover el intercambio de datos, información, software público, así como la colaboración en el desarrollo de proyectos de digitalización entre entidades.

i) Gestionar, mantener y documentar el Modelo de Gestión Documental (MGD), Modelo de Datos Abiertos Gubernamentales y Sistema de Gestión de Seguridad de la Información (SGSI) de la entidad.
j) Promover la conformación de equipos multidisciplinarios ágiles para la implementación de proyectos e iniciativas de digitalización de manera coordinada con los responsables de órganos y unidades orgánicas de la entidad.
k) Otras funciones que se le asigne en el ámbito de su competencia y aquellas concordantes con la materia.

2. Oficial de Seguridad de la información

Coordinador del plan de implementación del SGSI en el IGP. Tiene como responsabilidades:

a) Liderar la creación y revisión de las políticas, normas técnicas, directivas, reglamentos, procesos, procedimientos, manuales, instructivos, lineamientos, metodologías y planes referidos a la seguridad de la información.
b) Supervisar el cumplimiento de las políticas, procedimientos y controles de seguridad de la información.
c) Coordinar con los propietarios y custodios de la información para la elaboración del inventario de activos de la información y ejecución de la gestión de riesgos.
d) informar los resultados de su gestión al Comité de Gobierno Digital.
e) Dar seguimiento a los incidentes de seguridad de la información. evaluar riesgos y eventuales impactos.
f) Evaluar, coordinar y monitorear la implementación de los controles relacionados al SGSI.
g) Supervisar y apoyar en la difusión de los temas de seguridad de la información.
h) Supervisar la ejecución de las actividades que se deriven de los informes de las auditorias en seguridad de la información.
i) Las funciones específicas consignadas en la Resolución de Presidencia N° 052-IGP/2016.

3. OTIDG

   Oficina responsable de velar por el cumplimiento de los controles derivados de la Política de la Seguridad de la Información, en el ámbito de sus competencias.

4. Propietarios de la información

   Son los responsables de la información que se genera y se utiliza en las operaciones de su Unidad Orgánica. Tienen como responsabilidades:

   a) Participar en la identificación de los activos de información y en las actividades de análisis, evaluación y tratamiento de riesgos,
   b) Revisión periódica de la clasificación y etiquetado de la información con el propósito de verificar que cumpla con los requerimientos de la Entidad.
   c) Sugerir y apoyar en la elaboración de lineamientos y procedimientos de seguridad de la información dentro de sus respectivas áreas y procesos.
   d) Revisar periódicamente los niveles de acceso a los sistemas de información a su cargo.
   e) Supervisar y verificar la aplicación de los controles de seguridad con el custodio de la información.

5. Custodios de la información

   Son los encargados de la administración diaria de la seguridad de los activos de información y el monitoreo del cumplimiento de las políticas y los controles de seguridad en los activos de información que se encuentren bajo su administración, y tiene como responsabilidades:

   a) Administrar los controles relevantes a la seguridad de la información, acorde a las medidas de tratamiento de la información especificadas por los propietarios de la información (restricción de accesos, validación de autenticidad, mecanismos de resguardo, otros).
   b) Cumplir con los controles implementados para la protección de los activos de información asignados para su custodia.
   c) Colaborar en la investigación de los incidentes de seguridad de la información
   d) Identificar oportunidades de mejora y comunicarles al Oficial de Seguridad de la
      Información.

6. Usuarios

   Es el personal del IGP indistintamente del régimen laboral, modalidad de contratación o nivel jerárquico; así como por las personas naturales o jurídicas que prestan servicios, quienes utilizan la información en actividades habituales y se encuentran obligados a respetar las normas establecidas por la institución Tienen como responsabilidades:

   a) Cumplir con las políticas, lineamientos y procedimientos de seguridad de la información.
   b) Mantener la confidencialidad de las contraseñas para el acceso a aplicaciones, sistemas de información y recursos informáticos.

c) Utilizar la información del IGP únicamente para los propósitos autorizados,
d) Participar en los entrenamientos, capacitación y programas de sensibilización en temas de seguridad de la información.
e) Reportar cualquier incidente, potencial incidente u oportunidades de mejora de seguridad de la información.

7. Auditor Líder

Es el encargado de encabezar al equipo de auditores internos. Tiene como responsabilidades:

a) Convocar y realizar la reunión de apertura de auditoría.
b) Realizar la reunión de cierre de acuerdo al plan de auditoría.
c) Planificar y dirigir todas las actividades de la auditoría.
d) Ser independiente del área o proceso comprendido dentro del alcance de la auditoría, no auditar su propio trabajo.

8. Auditor interno

Es el responsable de preparar y llevar a cabo el proceso de auditoría interna para determinar el grado en el cual el sistema de gestión de seguridad de la información cumple con los requisitos de la Norma ISO/IEC 27001:2013. Tiene como responsabilidades:

a) Revisar la documentación y evidencias de cumplimiento dentro del alcance del
SGSI.
b) Llevar a cabo las reuniones de relevamiento de información con el personal involucrado, para corroborar o extender sus indagaciones.
c) Mantener imparcialidad, objetividad y ser independiente del área o proceso comprendido dentro del alcance de la auditoría, no auditar su propio trabajo.
d) Otras funciones en el ámbito de su competencia

9. Auditado

El auditado es cualquier personal del IGP que se encuentra sujeto a una revisión por parte del equipo de auditores. Tiene como responsabilidad proporcionar al equipo auditor la información necesaria y objetiva dentro del ámbito de sus competencias organizacionales y en función de los procesos donde participa, para asegurar un proceso de auditoría eficiente y eficaz.