Anexo I

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

1. Comité de Gobierno y Transformación 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 y Confianza Digital.
- El Jefe de la Oficina de Asesoría Jurídica.
- El Jefe de la Oficina de Planeamiento y Presupuesto.
- El Jefe de la Oficina de Administración.

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 públicas.

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 y Confianza Digital

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

a) Coordinar y reportar al Comité de Gobierno y Transformación Digital institucional la implementación, mantenimiento, y la aplicación de las normas relacionadas a seguridad digital, confianza digital, transformación digital, y gobierno digital.

b) Coordinar con el Líder de Gobierno y Transformación Digital el despliegue de las acciones reactivas y proactivas, e iniciativas para la transformación digital basada en seguridad digital de la entidad.

c) Coordinar con el Oficial de Gobierno de Datos y el Oficial de Datos Personales en todas las cuestiones relativas al uso ético de las tecnologías digitales y datos; y la protección de los datos personales en la entidad, respectivamente.

d) Coordinar con los dueños de los procesos o en su defecto con los responsables de las unidades de organización de la entidad toda iniciativa de mejora relacionado con la seguridad digital bajo su gestión.

e) Promover y desarrollar una cultura de seguridad digital en los funcionarios y servidores de la entidad, así como en el ciudadano en general, todo ello de manera coordinada con el Comité de Gobierno y Transformación Digital

f) Asistir, en su calidad de miembro del Comité de Gobierno y Transformación Digital, a en la correcta orientación, dirección, evaluación, monitoreo, control, y mejora continua en temas relacionados a la seguridad digital en la entidad; del mismo modo, en la definición e implementación de acciones, técnicas, estratégicas, coordinación y de respuesta ante incidentes de seguridad digital

g) Formular, articular, supervisar y coordinar la implementación, mantenimiento y mejora del SGSI.

h) Proponer lineamientos, estándares, directivas, guías y otros documentos en materia de seguridad y confianza digital.

i) Identificar, analizar, gestionar y minimizar los riesgos de seguridad digital y/o seguridad de la información.

j) Coordinar con la unidad de organización competente de la entidad programas, cursos, talleres u otras acciones de capacitación y

sensibilización en seguridad digital, ciberseguridad o seguridad de la información.

k) Promover el intercambio de conocimientos en materia de seguridad, confianza y transformación digital.

l) Garantizar la disponibilidad, integridad y confidencialidad de la información, generando la confianza digital en la entidad.

m) Asegurar que las adquisiciones de tecnología, desarrollo de software y servicios prestados por terceros cumplan los requisitos de seguridad de la información establecidos de acuerdo con la política de seguridad digital y/o seguridad de la información institucional aprobada.

n) Mantener informadas a las entidades competentes lo relacionado a la seguridad digital.

o) Informar al Centro Nacional de Seguridad Digital (CNSD) sobre los resultados y avances de seguridad y confianza digital, incidentes de seguridad digital, y otros dispuestos por el CNSD.

3. Equipo de Gestión de Seguridad de la Información

El equipo de Gestión de Seguridad de la información en cumplimiento de la norma vigente en materia de seguridad digital tiene como responsabilidad realizar las siguientes actividad en coordinación con el OSCD:

a) Implementar políticas y procedimientos relacionados a la Seguridad de la Información en coordinación con el OSCD.
b) Desarrollar y ejecutar planes de mitigación de riesgos para preservar la integridad, disponibilidad y confidencialidad de la información.
c) Garantizar el cumplimiento normativo y promover una cultura de seguridad de la información.
d) Fomentar una cultura de seguridad de la Información dentro de la organización a través de campañas de concienciación.
e) Realiza seguimiento a mejoras y no conformidades en seguridad de la información derivadas de auditorías.
f) Actividades adicionales asignadas por el Oficial de Seguridad y Confianza Digital, referentes seguridad de la información.

4. Oficina de Tecnologías de la Información y Datos Geofísicos

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.

5. 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.

6. 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 y Confianza Digital.

7. 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.

8. 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.

9. 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 27001:2022. 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

10. Equipo Auditor

Uno o más auditores que llevan a cabo una auditoría con el apoyo, si es necesario, de expertos técnicos estos tienen como responsabilidad de garantizar que la información cumple con los requisitos de la Norma ISO/IEC 27001:2022. Tiene como responsabilidades:

a) Apoyar en la Revisar la documentación y evidencias de cumplimiento dentro del alcance del Sistema de gestión y seguridad e la información.
b) Apoyar a la planificación de la auditoría acorde al programa de auditoría aprobado.
c) Apoyar en la reunión de apertura y cierre.

11. 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.