IGP V.B.
Firmado digitalmente por: TOVALINO YAPIAS Ivan James FAU 20131367008 soft
Motivo: Doy V° B°
Fecha: 29/10/2020 16:48:37-0500

IGP V.B.
Firmado digitalmente por: DELGADO ORTEGA Edgar FAU 20131367008 hard
Motivo: Doy V° B°
Fecha: 29/10/2020 17:31:06-0500

IGP V.B.
Firmado digitalmente por: BUENO CANO Raul Javier FAU 20131367008 soft
Motivo: Doy V° B°
Fecha: 29/10/2020 17:43:21-0500

REPÚBLICA DEL PERÚ

INSTITUTO GEOFÍSICO DEL PERÚ

Resolución de Presidencia

N° 088-IGP/2020

Lima, 29 de Octubre del 2020

VISTOS:

El Informe Legal N° 096-2020-IGP/GG-OAJ, Informe N° 033-2020-IGP/GG-OTIDG y el Informe N° 0183-2020-IGP/GG-OPP; y

CONSIDERANDO:

Que, mediante el Decreto Legislativo N° 136, se crea el Instituto Geofísico del Perú (IGP) como un Organismo Descentralizado del Sector Educación, cuya finalidad es la investigación científica, la enseñanza, la capacitación, la presentación de servicios y, la realización de estudios y proyectos, en las diversas áreas de la Geofísica;

Que, la Primera Disposición Complementaria Final del Decreto Legislativo N° 1013, Ley de Creación, Organización y Funciones del Ministerio del Ambiente, dispone la adscripción del IGP como un organismo público ejecutor del Ministerio del Ambiente;

Que mediante el Decreto Supremo N° 001-2015-MINAM, se aprobó el Reglamento de Organización y Funciones (ROF) del Instituto Geofísico del Perú (IGP);

Que, el numeral 1 de la Décima Séptima Disposición Complementaria Final del Decreto de Urgencia N° 021-2020 establece que el Instituto Geofísico del Perú es el Ente Rector de las investigaciones teóricas y aplicadas en la Ciencia Geofísica orientada a la ejecución de la Política Nacional de Gestión del Riesgo de Desastres;

Que, es necesario precisar que de acuerdo al Cuadro N° 2. Tipo de Documento de la Directiva DI 001-2020-IGP Aprobación, Modificación o Derogación de Documentos Normativos, aprobada mediante Resolución de Gerencia General N° 029-IGP/2020, de fecha 16 de octubre de 2020, las políticas de una entidad son aprobadas mediante Resolución de Presidencia Ejecutiva;

Que, mediante el Informe N° 033-2020-IGP/GG-OTIDG, la Jefa de la Oficina de Tecnologías de la Información y Datos Geofísicos explicó los motivos para que se apruebe la Política de Seguridad de la Información; en ese sentido, indicó que el beneficio que tendrá el IGP es que podrá disponer de una herramienta que le permitirá gestionar la Seguridad de la Información en las actividades de la institución;

Que, en el Informe N 0183-2020-IGP/GG-OPP, se indica lo siguiente:

"La Política propuesta, cumple con los 4 principios que debe contar todo documento normativo: Eficacia, Simplicidad, Suficiencia; y, ser un Proceso Sistémico, el procedimiento es de carácter permanente y operativo, toda vez que se desarrolla de forma constante y se encuentra vinculada con las funciones de apoyo del IGP, La información contenida en la propuesta es clara, sencilla y secuencial y el desarrollo de la información es bajo un enfoque por procesos (secuencial y transversal)";

Que, de la revisión del citado Informe N° 0183-2020-IGP/GG-OPP se advierte que cumple con la normativa y considerando que el IGP podrá disponer de una herramienta que le permitirá gestionar la Seguridad de la Información en las actividades de la institución, es viable la aprobación de la Política de Seguridad de la Información propuesta por la Jefa de la Oficina de Tecnologías de la Información y Datos Geofísicos;

Que, mediante Informe Legal N° 093-2020-IGP/GG-OAJ se emitió opinión legal favorable para aprobar la Política de Seguridad de la Información;

Con el visado de la Gerencia General, de la Oficina de Asesoría Jurídica, de la Oficina de Tecnología de Información y Datos Geofísicos y de la Oficina de Planeamiento y Presupuesto, y;

De conformidad con el Decreto Supremo N° 001-2015-MINAM y la Directiva DI 001-2020-IGP Aprobación, Modificación o Derogación de Documentos Normativos, aprobada mediante Resolución de Gerencia General N° 029-IGP/2020;

SE RESUELVE:

Artículo 1.- Aprobar la Política de Seguridad de la Información del Instituto Geofísico del Perú, que como anexo forma parte integrante de la presente Resolución de Presidencia.

Artículo 2.- Deróguese cualquier documento que se oponga a la Política de Seguridad de la Información, aprobada en el Artículo 1 de la presente Resolución de Presidencia.

Artículo 3.- Disponer la publicación de la presente Resolución de Presidencia en el Portal Institucional del Instituto Geofísico del Perú (www.gob.pe/igp).

Regístrese, comuníquese y cúmplase.

Dr. Hernando Tavera Huarache
Presidente Ejecutivo

IGP
Firmado digitalmente por: TAVERA HUARACHE Hernando Jhonny FAU 20131367008 hard
Motivo: Soy el autor del documento
Fecha: 29/10/2020 18:33:11-0500

POLÍTICA PO 002-2020-IGP

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Versión 01

POLÍTICA PO 002-2020-IGP

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

VERSIÓN	FECHA	DESCRIPCIÓN
1	15/Sep/2020	Documento Inicial
FORMULADO **OFICINA DE TECNOLOGÍA DE LA INFORMACIÓN Y DATOS GEOFÍSICOS**	**REVISADO Y VISADO** **OFICINA DE PLANEAMIENTO Y PRESUPUESTO**	**REVISADO Y VISADO** **OFICINA DE ASESORÍA JURÍDICA**
IGP Firmado digitalmente por: LUNA GUZMAN Maria Rosa FAU 20131367008 hard Motivo: Soy el Autor del Documento Fecha: 29/10/2020 16:54:17-0500		
APROBADO **PRESIDENCIA EJECUTIVA**	**REVISADO Y VISADO** **(DENOMINACIÓN DE ORGANO/UNIDAD ORGANICA)**	**REVISADO Y VISADO** **(DENOMINACIÓN DE ORGANO/UNIDAD ORGANICA)**

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

I. OBJETIVO

Proporcionar orientación general y apoyo de la alta dirección a la gestión de la seguridad de la información en concordancia con los requisitos de la institución y con las regulaciones y leyes pertinentes.

II. BASE LEGAL

- Ley Nº 29733 Ley de Protección de Datos Personales
- Resolución N° 129-2014/CNB-INDECOPI – que aprueba 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".
- Resolución Ministerial Nº 004-2016-PCM que 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.
- Resolución Ministerial Nº 087-2019-PCM que aprueba disposiciones sobre la conformación y funciones del Comité de Gobierno Digital.
- Resolución de Presidencia N° 036-IGP/2020 que conforma y establece las funciones del Comité de Gobierno Digital.
- Resolución de Presidencia N° 052-IGP/2016 que designa como Oficial de Seguridad de la Información (OSI) al Jefe de la Oficina de tecnologías de la Información y Datos Geofísicos del IGP.

III. ALCANCE

La Política de Seguridad de la Información tiene alcance a todas las unidades orgánicas y a todos los servidores, funcionarios y proveedores de servicios que tengan acceso o que desarrollen, adquieran o usen sistemas de información o datos del IGP.

IV. PRINCIPIOS

a) **Confidencialidad:** Propiedad de que la información no esté disponible o sea revelada a personas, entidades o procesos no autorizados.
b) **Integridad:** Propiedad de que la información sea exacta y completa, libre de modificaciones no autorizadas.
c) **Disponibilidad:** Propiedad de la información de ser accesible y utilizable por petición de una entidad autorizada.
d) **Autenticidad:** Propiedad de que una entidad es lo que es dice ser.
e) **No repudio:** Capacidad de probar la ocurrencia de un evento o acción reivindicada y sus entidades originarias.

V. POLÍTICAS

El IGP es un Organismo Público Ejecutor del Ministerio del Ambiente, actúa como organismo competente para realizar investigación científica, enseñanza y capacitación, monitoreo, prestación de servicios, desarrollo tecnológico y la realización de estudios y proyectos; en las diversas áreas de la geofísica, para contribuir con la gestión de riesgos de desastres a nivel nacional. Mediante la presente política se compromete a:

- Establecer, implementar, mantener y mejorar continuamente un Sistema de Gestión de la Seguridad de la Información (SGSI)
- Satisfacer los requisitos del marco legal institucional, políticas y normas adoptadas relacionadas con la seguridad de la información.
- Evaluar los riesgos de seguridad de la información y determinar su tratamiento a través de un conjunto de controles.
- Proteger la confidencialidad, integridad y disponibilidad de la información utilizada para ejercer las competencias institucionales, independientemente del medio en el que se soporta, a través de la implementación de los controles aplicables seleccionados.
- Establecer objetivos de seguridad de la información medibles con base en los requisitos aplicables y los resultados de la evaluación y tratamiento de riesgos, con enfoque en activos de información prioritarios.

VI. LINEAMIENTOS DE POLITICA

La presente Política de Seguridad de la Información es de carácter general. Para asegurar su cumplimiento se establecerán los lineamientos de seguridad de la información a través de distintos tipos documentales como procedimientos y lineamientos, los cuales contendrán políticas específicas y los controles que permitirán lograr los objetivos de la seguridad de la información del IGP.

VII. ESTRATEGIA

Aunque la política tiene un alcance general en la institución, su aplicación formal se llevará a cabo de acuerdo con el alcance especificado para el SGSI, el cual es ampliable en el tiempo. El alcance inicial del SGSI se especifica en el **Anexo I Determinación del Alcance del Sistema de Gestión de la Seguridad de la Información**.

La presente política es desplegada en Objetivos de la Seguridad de la Información, consignados en el **Anexo II Objetivos de la Seguridad de la Información**. A su vez, se utilizará la estrategia de utilizar un tablero de control para estos objetivos y asignar indicadores a cada uno, de modo que estos sean medibles y se puedan asignar recursos, responsabilidades, actividades, plazos y formas de evaluar los resultados.

Para el correcto despliegue de la presente política, se han recopilado y establecido responsabilidades con base en las necesidades del SGSI y de funciones previamente establecidas; esto se consigna en el **Anexo III Roles y Responsabilidades Generales del Sistema de Gestión de la Seguridad de la Información**.

VIII. GLOSARIO DE TÉRMINOS

Definiciones de términos que requieren ser explicados o detallados, para una mejor comprensión, debe tenerse en cuenta que un mismo término puede tener diferentes implicancias en documentos normativos diferentes.

- **IGP:** Instituto Geofísico del Perú
- **SGSI:** Sistema de Gestión de la Seguridad de la Información
- **CGD:** Comité de Gobierno Digital.
- **OTIDG:** Oficina de Tecnología de Información y Datos Geofísicos
- **Control:** Medida que modifica un riesgo. Los controles incluyen cualquier proceso, la política, dispositivo, práctica, u otras acciones que modifiquen un riesgo. Los controles no siempre pueden proporcionar el efecto de modificación previsto o asumido.
- **Seguridad de la información:** Preservación de la confidencialidad, la integridad y la disponibilidad de la información. Además, otras propiedades, como la autenticidad, la responsabilidad, el no repudio, y confiabilidad también pueden estar involucrados.
- **Sistema de Gestión de Seguridad de la Información (SGSI):** Consiste en un conjunto de políticas, procedimientos, guías y sus recursos y actividades asociados, que son gestionados de manera colectiva por una organización. Un SGSI es un enfoque sistemático para establecer, implementar, operar, monitorizar, revisar, mantener y mejorar la seguridad de la información de una organización para alcanzar los objetivos del negocio. Este enfoque está basado en una apreciación del riesgo y en los niveles de aceptación del riesgo de la organización diseñados para tratar y gestionar con eficacia los riesgos. El análisis de los requisitos para la protección de los activos de información, según sea necesario, contribuye a la exitosa implementación de un SGSI.

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.