



INSTITUTO GEOFÍSICO DEL PERÚ

Resolución de Gerencia General

N° 059-IGP/2022

Lima, 20 de Diciembre del 2022

VISTOS:

El Informe N° 00005-2022-IGP/GG-OSI, el Informe N° 0244-2022-IGP/GG-OPP y el Informe Legal N° 174-2022-IGP/GG-OAJ; 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 prestación 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, Decreto Legislativo que aprueba la 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, mediante Resolución de Gerencia General N° 029-IGP/2020, se aprobó la Directiva DI 001-2020-IGP, denominada: "Aprobación, modificación o derogación de documentos normativos";

Que, el numeral 7.2.1 de la Directiva DI 001-2020-IGP, "Aprobación, modificación o derogación de documentos normativos del IGP", aprobada mediante Resolución Gerencial N° 029-IGP/2020, establece la jerarquía funcional de los documentos normativos disponiendo que los PROCEDIMIENTOS y LINEAMIENTOS se encuentran en los niveles 4 y 6 respectivamente, en concordancia con los numerales 7.2.2.9 y 7.2.2.12 que indica sobre los procedimientos y lineamientos que: *"Es la descripción documentada de cómo deben ejecutarse las actividades que conforman un proceso, tomando en cuenta los elementos que la componen y su secuencialidad, permitiendo de esta manera una operación coherente. Cada procedimiento tiene una codificación única y se aprueba mediante acto administrativo de manera individual"*

o conjunta, y se incorporan al Manual de Procedimientos”; y, “Instrumentos donde se establecen los términos, límites y características que deben observarse para actividades o procedimientos de la institución”;

Que, en el presente caso la aprobación de la actualización/modificación del Lineamiento LI 001-2020-IGP denominado: “Lineamiento de Seguridad de la Información” y del Procedimiento PR 005-2020-IGP denominado: “Seguimiento, Medición, Gestión del Cambio y Revisión por la Dirección”, se debe realizar a través de una Resolución de Gerencia General, conforme a la Jerarquía Funcional prevista en la Directiva DI N° 001-2020-IGP;

Que, a través del Informe N° 00005-2022-IGP/GG-OSI, la Oficial de Seguridad de la Información remite la propuesta de actualización/modificación del Lineamiento LI 001-2020-IGP denominado: “Lineamiento de Seguridad de la Información” y del Procedimiento PR 005-2020-IGP denominado: “Seguimiento, Medición, Gestión del Cambio y Revisión por la Dirección”;

Que, mediante el Informe N° 0244-2022-IGP/GG-OPP, la Oficina de Planeamiento y Presupuesto emite opinión técnica favorable para que se apruebe la propuesta de actualización/modificación del Lineamiento LI 001-2020-IGP denominado: “Lineamiento de Seguridad de la Información” y del Procedimiento PR 005-2020-IGP denominado: “Seguimiento, Medición, Gestión del Cambio y Revisión por la Dirección”; señalando que dichas propuestas se encuentran alineadas a la Directiva DI 001-2020-IGP “Aprobación, Modificación o Derogación de Documentos Normativos”;

Que, a través del Informe Legal N° 174-2022-IGP/GG-OAJ, la Oficina de Asesoría Jurídica emitió opinión legal favorable para que se apruebe la actualización/modificación del Lineamiento LI 001-2020-IGP denominado: “Lineamiento de Seguridad de la Información” y del Procedimiento PR 005-2020-IGP denominado: “Seguimiento, Medición, Gestión del Cambio y Revisión por la Dirección”;

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

De conformidad con lo dispuesto en el Decreto Legislativo N° 136, Ley del Instituto Geofísico del Perú, el Reglamento de Organización y Funciones del Instituto Geofísico del Perú, aprobado por Decreto Supremo N° 001-2015-MINAM, el Decreto Legislativo N° 1013, Decreto Legislativo que aprueba la Ley de Creación, Organización y Funciones del Ministerio del Ambiente, que dispone la adscripción del Instituto Geofísico del Perú (IGP) como Organismo Público Ejecutor del Ministerio del Ambiente y la Directiva DI 001-2020-IGP, que dispone los lineamientos para la “Aprobación, modificación o derogación de documentos normativos”, aprobada mediante Resolución de Gerencia General N° 029-IGP/2020.

SE RESUELVE:


Artículo 1.- Aprobar la actualización/modificación de los siguientes documentos normativos que como anexo forman parte integrante de las presente Resolución Gerencia General:

- Lineamiento LI 001-2020-IGP denominado: "Lineamiento de Seguridad de la Información".
- Procedimiento PR 005-2020-IGP denominado: "Seguimiento, Medición, Gestión del Cambio y Revisión por la Dirección".

Artículo 2.- Disponer la publicación de la presente Resolución de Gerencia General en el Portal Institucional del Instituto Geofísico del Perú (www.gob.pe/igp).


Regístrese, comuníquese y cúmplase.

Javier Bueno Cano
Gerente General

	LINEAMIENTO	Versión: 04
	LINEAMIENTO DE SEGURIDAD DE LA INFORMACIÓN	Código: LI 001-2020-IGP Sigla de Área: OTIDG

LINEAMIENTO LI 001-2020-IGP --- **LINEAMIENTO DE SEGURIDAD DE LA INFORMACIÓN**


Versión 04

	LINEAMIENTO	Versión: 04
	LINEAMIENTO DE SEGURIDAD DE LA INFORMACIÓN	Código: LI 001-2020-IGP Sigla de Área: OTIDG


LINEAMIENTO LI 001-2020-IGP

LINEAMIENTO DE SEGURIDAD DE LA INFORMACIÓN

VERSIÓN	FECHA	DESCRIPCIÓN
01	05/12/2020	1. Documento Inicial
02	06/08/2021	1. Se incluye en la política (5.3) la referencia para la clasificación y manejo de activos y se agrega el anexo v. 2. Se agrega a la política (5.10.2 e) el requisito de notificar debilidades de SI.
03	05/07/2022	1. Se precisa la definición de Información del anexo V. 2. Se modifica esquema de clasificación del anexo V. 3. se añade cuadro controles aplicables en el anexo V.
04	07/11/2022	1. Se actualiza la Política de Gestión de Seguridad de Activos de Información. 2. Se modifica la Gestión de acceso del personal contenidas dentro de la Política de Control de Acceso. 3. Se añaden las políticas de control criptográfico. 4. modificación de la Política de Seguridad Física y del Entorno 5. Se añade la política de Escritorio y pantalla limpia de información. 6. Se han identificado los controles de la DDA dentro del cuadro de Controles Aplicables para Los Activos de Información.

	LINEAMIENTO	Versión: 04
	LINEAMIENTO DE SEGURIDAD DE LA INFORMACIÓN	Código: LI 001-2020-IGP Sigla de Área: OTIDG

FORMULADO OFICINA DE TECNOLOGIAS DE LA INFORMACIÓN Y DATOS GEOFISICOS	REVISADO Y VISADO OFICINA DE PLANEAMIENTO Y PRESUPUESTO	REVISADO Y VISADO OFICINA DE ASESORIA JURIDICA
APROBADO GERENCIA GENERAL		

	LINEAMIENTO	Versión: 04
	LINEAMIENTO DE SEGURIDAD DE LA INFORMACIÓN	Código: LI 001-2020-IGP Sigla de Área: OTIDG

LINEAMIENTO DE SEGURIDAD DE LA INFORMACIÓN


I. OBJETIVO

El Lineamiento de Seguridad de la Información tiene como objetivo salvaguardar los activos de información del IGP y los sistemas de información que soportan su procesamiento, frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de minimizar los riesgos de daño y asegurar la confidencialidad, integridad y disponibilidad de la información; así como también garantizar la continuidad de los sistemas de información vinculados.

Asimismo, a través de la implementación del presente lineamiento, se busca que la Seguridad de la Información se incorpore como parte de la cultura organizacional del IGP.

II. BASE LEGAL

- Decreto Legislativo N° 136 Ley de Creación del IGP
- Ley N° 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 N° 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 N° 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.

	LINEAMIENTO	Versión: 04
	LINEAMIENTO DE SEGURIDAD DE LA INFORMACIÓN	Código: LI 001-2020-IGP Sigla de Área: OTIDG

III. ALCANCE

Los Lineamientos de Seguridad de la información tienen alcance a todos los servidores/as, funcionarios/as y proveedores de servicio que tengan acceso o que desarrollen, adquieran o usen sistemas de información y/o datos del IGP. Comprende toda la información producida, manejada, transmitida, almacenada y propiedad del IGP; asimismo, todos los sistemas y datos asociados con el almacenamiento, procesamiento y transmisión de la información, generada por y a favor del IGP.

El presente documento comprende las siguientes políticas específicas de Seguridad de la Información:

- Política de Organización de la Seguridad de la Información.
- Política de Seguridad Relativa a los Recursos Humanos, de Formación y Concientización
- Política de Gestión de Seguridad de Activos de Información.
- Política de Control de Accesos,
- Política de Seguridad Física y del Entorno.
- Política de Seguridad de las Operaciones.
- Política de Seguridad de las Comunicaciones.
- Política de Adquisición, Desarrollo y Mantenimiento de Sistemas.
- Política de control criptográfico
- Política de Relación con Proveedores.
- Política de Gestión de Incidentes de Seguridad de la Información.
- Política de Continuidad de Seguridad de la información,
- Política de Cumplimiento de Protección y Privacidad de Datos Personales
- Política de Escritorio y pantalla limpia de información


IV. LINEAMIENTOS GENERALES

4.1. Política y objetivos de Seguridad de la Información

La política de nivel general que enmarca el presente lineamiento se encuentra documentada en **PO 002-2020-IGP Política de Seguridad de la Información**.

4.2. Sanciones por incumplimiento

El IGP se reserva el derecho de tomar medidas administrativas disciplinarias a los servidores que incumplan con lo dispuesto en el Lineamiento de Seguridad de la Información conforme a las disposiciones señaladas en los documentos normativos de la entidad, sin perjuicio de las acciones civiles y/o penales que pudieran corresponder.

	LINEAMIENTO	Versión: 04
	LINEAMIENTO DE SEGURIDAD DE LA INFORMACIÓN	Código: LI 001-2020-IGP Sigla de Área: OTIDG

V. LINEAMIENTOS ESPECÍFICOS

5.1. Política de Organización de la Seguridad de la Información

5.1.1. Objetivo

Establecer un marco de referencia de la gestión para iniciar y controlar la implementación y operación de la gestión de la seguridad de la información dentro de la entidad.

5.1.2. Política

(a) Roles y Responsabilidades:

El IGP debe definir roles y responsabilidades de Seguridad de la información para la protección de los activos de información, la gestión de riesgos de Seguridad de la información y la aceptación de los riesgos residuales, entre otras actividades específicas de seguridad de la información. Los roles se definen en los perfiles de puestos, en los contratos, en documentos normativos y/o documentos administrativos internos.

(b) Segregación de Funciones:


(i) El IGP debe segregar funciones para reducir oportunidades de modificación no autorizada o no intencional o mal uso de los activos de la organización. En el Reglamento de Organización y Funciones (ROF) el IGP consigna la segregación de funciones a partir de las unidades orgánicas.

(ii) Por otro lado, la designación de un Oficial de Seguridad de la Información (OSI) y el establecimiento del Comité de Gobierno Digital (CGD), que incluye al Oficial de Seguridad de la Información, confiere al IGP contar con entidades internas de control transversal con la participación directa de la alta dirección.

(c) Contacto con autoridades y grupos especiales de interés

(i) El IGP, a través del Oficial de Seguridad de la Información, del Equipo de Respuestas ante Incidentes de Seguridad Digital y del Comité de Gobierno Digital, mantendrá contacto con la Secretaría de Gobierno Digital (SeGD) de la Presidencia del Consejo de Ministros, con el Equipo de Respuesta ante Incidentes de Seguridad Digital Nacional (PeCERT) y Centro Nacional de Seguridad Digital, de acuerdo con los requerimientos en materia de seguridad de la información y de acuerdo con la normativa vigente correspondiente. Esto incluye la obligación de notificar al Centro Nacional de Seguridad Digital todo incidente de seguridad digital, implementada a través del Procedimiento Gestión de atenciones TIC y Eventos e Incidentes de Seguridad de la Información.

(ii) A raíz de la colaboración interinstitucional, el Oficial de Seguridad de la Información participará en los grupos de trabajo interinstitucionales Ad Hoc que se establezcan. Adicionalmente, la Jefe de la Oficina de Tecnologías de la Información y Datos Geofísicos impulsará el contacto y mutua

	LINEAMIENTO	Versión: 04
	LINEAMIENTO DE SEGURIDAD DE LA INFORMACIÓN	Código: LI 001-2020-IGP Sigla de Área: OTIDG


colaboración técnica con los proveedores especializados en servicios relacionados con la seguridad de la información.

(d) Seguridad de la Información en la gestión de proyectos:

- (i) La Oficina de Tecnologías de la Información y Datos Geofísicos del IGP en coordinación con la Oficina de Planeamiento y Presupuesto, deben gestionar que se integre la seguridad de la información en el proceso de gestión de proyectos de la Entidad, incluyendo todos los tipos de proyectos, para garantizar que los riesgos de seguridad de la información sean identificados y tratados pertinentemente.
- (ii) Los proyectos de inversión pública, en el marco del sistema nacional de programación multianual de inversiones, en la etapa de formulación de proyectos se debe incorporar una evaluación de riesgos de seguridad de la información para identificar los riesgos y determinar los controles necesarios. La evaluación de riesgos debe cubrir las etapas de formulación y evaluación, ejecución y funcionamiento del proyecto.
- (iii) Los proyectos de inversión pública en el marco del sistema nacional de programación multianual de inversiones, durante la elaboración del perfil del proyecto, así como el expediente técnico o documento equivalente, deben incorporar entre sus objetivos, objetivos de seguridad de la información del proyecto, alineados con los objetivos generales del sistema de gestión.
- (iv) Los proyectos de carácter interno que no son parte del sistema nacional de programación multianual de inversiones, en las etapas de diseño, implementación y operación se debe incorporar la evaluación de riesgos de SI. En la etapa del diseño del proyecto, se deberá hacer referencia a los objetivos del sistema de gestión de seguridad de la información con los que contribuye.

(e) Dispositivos Móviles:

- (i) El IGP utiliza dispositivos móviles institucionales y permite la utilización de dispositivos móviles de propiedad privada, bajo control y autorización. En cualquier caso, el IGP, a través de la Oficina de Tecnologías de la Información y Datos Geofísicos, realizará el monitoreo de la actividad en los dispositivos móviles, por ejemplo, los intentos fallidos de autenticación.
- (ii) La Oficina de Tecnologías de la Información y Datos Geofísicos del IGP es responsable de autorizar a los servidores y a los proveedores de servicio sobre el uso de dispositivos móviles en las instalaciones del IGP y sobre la instalación y uso de aplicaciones y servicios del IGP en dispositivos móviles de su propiedad, que sean necesarios para la prestación del servicio.
- (iii) Toda asignación de dispositivos móviles institucionales será justificada, requerida y aprobada por la jefatura de la unidad orgánica correspondiente, con el posterior Vo Bo de la Oficina de Tecnologías de la Información y Datos Geofísicos; la asignación será documentada en registros.
- (iv) Todo dispositivo móvil institucional o de propiedad de personas naturales que se apruebe para utilizarse con servicios o aplicaciones del IGP, deberá implementar algún método de autenticación para el acceso.
- (v) Los servidores que no cuenten con un teléfono móvil institucional y requieran utilizar la cuenta de correo electrónico del IGP en sus teléfonos

	LINEAMIENTO	Versión: 04
	LINEAMIENTO DE SEGURIDAD DE LA INFORMACIÓN	Código: LI 001-2020-IGP Sigla de Área: OTIDG

personales, deberán requerir a la Oficina de Tecnologías de la Información y Datos Geofísicos con el VoBo previo de la jefatura de la unidad orgánica a la que pertenecen.

(vi) Para cualquier aplicación o servicio del IGP que se utilice en dispositivos móviles institucionales o de propiedad privada, los usuarios deberán firmar un acuerdo de usuario final en el que reconocen sus obligaciones y aceptan que la institución puede ejercer monitoreo a las actividades realizadas.

(vii) Las actividades de instalación y configuración de las aplicaciones de los dispositivos móviles son realizadas por La Oficina de Tecnologías de la Información y Datos Geofísicos del IGP. Se debe verificar la configuración de seguridad de los dispositivos móviles según **Anexo I Checklist de configuración de seguridad de dispositivos móviles**.

(viii) El servidor del IGP debe proteger sus dispositivos móviles, no debiendo entregarlos a otra persona, en particular en aquellos dispositivos inteligentes que pueden acceder a información interna o confidencial de la entidad. En estos casos, incluso los mensajes recibidos de números o remitentes desconocidos deben ser denegados y borrados sin ser abiertos. Los servidores deben evitar utilizar redes inalámbricas públicas o desconocidas.

(ix) El IGP no emplea los dispositivos móviles para almacenar información directamente, por lo que no serán sometidos a copias de respaldo.

(x) Los siguientes dispositivos móviles institucionales tienen la prohibición de retirarse del perímetro de la sede institucional a la cual están asignados:

1. Teléfono móvil asignado a CENSIS.

(xi) El IGP a través de La Oficina de Tecnologías de la Información y Datos Geofísicos, debe mantener una administración centralizada de las características de los dispositivos móviles y las aplicaciones instaladas en ellos que procesan o almacenan información crítica.

(xii) En caso de pérdida o robo de dispositivos móviles institucionales, se debe proceder de la siguiente manera:


1. El usuario debe reportar el hecho tan pronto sea posible a OTIDG (en todos los casos) y a Control Patrimonial (en caso de dispositivos propiedad del IGP).
2. reportar la pérdida o robo de acuerdo a la DI-004-2020-IGP Directiva de Normas de austeridad y uso del servicio de telefonía móvil institucional.

(xiii) En caso de pérdida o robo de dispositivos móviles de propiedad privada que hayan sido autorizados para utilizar el correo institucional, se debe proceder de la siguiente manera:


1. El usuario debe reportar el hecho tan pronto sea posible a OTIDG.
2. El personal de OTIDG eliminará el contenido del correo electrónico institucional del equipo, a través de la consola de control del correo electrónico.

(f) Trabajo remoto:

(i) El IGP emplea el trabajo remoto para acceder y procesar información, más no ha previsto almacenar información en sitios de trabajo remoto para usuarios finales.

	LINEAMIENTO	Versión: 04
	LINEAMIENTO DE SEGURIDAD DE LA INFORMACIÓN	Código: LI 001-2020-IGP Sigla de Área: OTIDG

- (ii) El trabajo remoto está normado en detalle en el documento LI-003-2020-IGP/GG OAD Lineamiento Para la Aplicación de Trabajo Remoto de Los Servidores Civiles Del Instituto Geofísico Del Perú.
- (iii) El trabajo remoto puede ser activado ante la aplicación de protocolos sanitarios que exijan el distanciamiento social o por necesidad de las unidades orgánicas, en cuyo caso, el jefe inmediato requerirá a la Unidad de Recursos Humanos, la modificación del lugar de prestación de servicios, variando el centro de labores habitual de trabajo al domicilio. La comunicación que la Unidad de Recursos Humanos emite al servidor debe ser notificada a la Oficina de Tecnologías de la Información y Datos Geofísicos del IGP, para la activación de los controles de seguridad de la información correspondientes.
- (iv) En el caso de utilizar dispositivos móviles, se aplicará la política específica de dispositivos móviles del presente documento.
- (v) La Oficina de Tecnologías de la Información y Datos Geofísicos del IGP brindará asesoramiento a los servidores en cuanto a la configuración de redes domésticas y configuración de servicios de red inalámbricos de modo que se maximice el nivel de seguridad.
- (vi) El servidor deberá tramitar una solicitud para la configuración de acceso a VPN a través de la Oficina de Tecnologías de la Información y Datos Geofísicos del IGP.
- (vii) El ancho de banda mínimo para viabilizar el trabajo remoto es de 4Mbps.

	LINEAMIENTO	Versión: 04
	LINEAMIENTO DE SEGURIDAD DE LA INFORMACIÓN	Código: LI 001-2020-IGP Sigla de Área: OTIDG

5.2. Política de Seguridad Relativa a los Recursos Humanos de Formación y de Concientización

5.2.1. Objetivo

Asegurar una correcta gestión de los recursos humanos en el IGP, siendo los servidores parte fundamental del resguardo de la Seguridad de la información.


5.2.2. Política

(a) Antes del Empleo – Selección, Términos y Condiciones Laborales

- (i) La Unidad de Recursos Humanos del IGP, debe verificar y registrar los antecedentes laborales y las competencias requeridas para el puesto, según el procedimiento Selección y Contratación de Personal y utilizando las herramientas gubernamentales a disposición, como la Plataforma Nacional de Interoperabilidad del Estado – PIDE. Esto incluye la consulta y recuperación de registros de:
 1. antecedentes policiales, penales y judiciales.
 2. Registro Nacional de Sanciones de Destitución y Despidos (RNSDD)
 3. REDAM Registro Nacional de Deudores Alimentarios
 4. Registro de Grados y Títulos - SUNEDU
- (ii) La Unidad de Recursos Humanos del IGP aplicará los criterios de selección establecidos para detener el proceso de contratación o continuar con el mismo de acuerdo con la información de los registros consultados.
- (iii) Para el caso de los cargos de confianza donde no se aplica el proceso de selección, se recupera la documentación de los mismos registros que se consultan en un proceso de selección y contratación; de observarse antecedentes desfavorables, se comunican a la alta dirección, quedando a su discreción cualquier acción posterior.
- (iv) La Unidad de Recursos Humanos del IGP, deberá establecer en los acuerdos contractuales de empleo, las cláusulas de confidencialidad respecto a la Seguridad de la Información, cláusula respecto a las leyes de derecho de autor o protección de datos, según corresponda.
- (v) La Unidad de Logística en el marco del procedimiento Contrataciones de bienes y servicios por montos menores o iguales a ocho UIT, incluirá en las O/C u O/S los compromisos de seguridad de la información necesarios, conservando la evidencia de la confirmación de la recepción.
- (vi) La Oficina de Tecnologías de la Información y Datos Geofísicos del IGP podrá generar declaraciones juradas de confidencialidad y compromiso con otras exigencias de seguridad de la información, por ejemplo, para personal de proveedores de servicios.


(b) Durante el Empleo – Responsabilidad de la Alta Dirección, Concientización y Capacitación, Proceso Disciplinario.

- (i) La alta dirección del IGP se asegura que los servidores del IGP y los proveedores sean instruidos oportunamente sobre sus roles y responsabilidades de seguridad de la información a través de las funciones de las unidades orgánicas correspondientes (Unidad de Recursos


	LINEAMIENTO	Versión: 04
	LINEAMIENTO DE SEGURIDAD DE LA INFORMACIÓN	Código: LI 001-2020-IGP Sigla de Área: OTIDG

Humanos, Unidad de Logística y la Oficina de Tecnologías de la Información y Datos Geofísicos).

- (ii) La alta dirección del IGP demuestra el apoyo a las políticas, los procedimientos, lineamientos y controles de seguridad de la información al suscribir los documentos normativos correspondientes. Adicionalmente, comunicará directamente a los servidores la importancia del cumplimiento de los requisitos a través de los canales institucionales.
- (iii) La Unidad de Recursos Humanos del IGP, debe comunicar a los servidores del IGP, sus responsabilidades con respecto a la Seguridad de la Información, siendo responsables de la Seguridad de la información a la que tienen acceso, según las funciones o actividades que realicen.
- (iv) La Unidad de Recursos Humanos del IGP, en coordinación con la Oficina de Tecnologías de la Información y Datos Geofísicos debe establecer programas de inducción para los nuevos servidores, así como, actualizaciones regulares sobre políticas, procedimientos y otros documentos normativos.
- (v) La Unidad de Recursos Humanos del IGP, debe comunicar a a Oficina de Tecnologías de la Información y Datos Geofísicos del IGP, cuando corresponda, el inicio, rotación del vínculo laboral de los servidores para el otorgamiento de acceso a los Sistemas de información.
- (vi) La Oficina de Tecnologías de la Información y Datos Geofísicos, en coordinación con la URH programará actividades de formación y capacitación en el marco del sistema de gestión de la seguridad de la información para asegurar que los colaboradores conozcan sus roles y responsabilidades, adquieran las competencias necesarias y se logre una cultura de prevención en seguridad de la información fortalecida. Esto será realizado en el marco del Procedimiento de Capacitación o a través de un Cronograma de Capacitación y Concientización propio de la Oficina de Tecnologías de la Información y Datos Geofísicos.
- (vii) La Unidad de Logística, en coordinación con la Oficina de Tecnologías de la Información y Datos Geofísicos, debe incluir en los Términos de Referencia de los productos y servicios más estrechamente relacionados con la seguridad de la información (como servicios de internet, firewall, servicios web) requisitos relacionados con actividades de formación técnica para los administradores de servicios, usuarios y dueños de activos de información del IGP.
- (viii) La Oficina de Tecnologías de la Información y Datos Geofísicos, en coordinación con el Oficial de Seguridad de la Información, incluirán actividades internas de formación y de concientización.
- (ix) La Oficina de Tecnologías de la Información y Datos Geofísicos en coordinación con la Unidad Funcional de Comunicaciones, complementarán las actividades de formación y concientización, con campañas audiovisuales de temas específicos, que utilicen un lenguaje sencillo, ejemplos y casos para atraer la atención de los usuarios.

	LINEAMIENTO	Versión: 04
	LINEAMIENTO DE SEGURIDAD DE LA INFORMACIÓN	Código: LI 001-2020-IGP Sigla de Área: OTIDG

- (x) La Unidad de Recursos Humanos del IGP, puede iniciar procesos disciplinarios y/o acciones legales pertinentes a los servidores que incumplan las políticas de seguridad de la información y disposiciones en los documentos normativos de seguridad de la información establecidos. En este caso, el inicio del proceso debe ser requerido por la Oficina de Tecnologías de la Información y Datos Geofísicos, tras verificar las evidencias de incumplimiento. Las referencias de estas evidencias deberán igualmente ser proporcionadas por la Oficina de Tecnologías de la Información y Datos Geofísicos. Las acciones a tomarse en los procesos disciplinarios deben utilizar las escalas indicadas en el Reglamento Interno de Servidores Civiles o documento análogo aplicable y deberán aplicarse los documentos normativos adicionales que se aprueben.
- (c) Después del Empleo
- (i) Las responsabilidades y deberes que permanecen válidos luego de la desvinculación se encuentran en los contratos.
 - (ii) La Unidad de Recursos Humanos del IGP, debe comunicar a La Oficina de Tecnologías de la Información y Datos Geofísicos del IGP, cuando corresponda, la finalización del vínculo laboral del servidor al día siguiente de tomado conocimiento de la culminación del vínculo laboral a fin de realizar la deshabilitación de los accesos a los sistemas de información y demás recursos.

	LINEAMIENTO	Versión: 04
	LINEAMIENTO DE SEGURIDAD DE LA INFORMACIÓN	Código: LI 001-2020-IGP Sigla de Área: OTIDG

5.3. Política de Gestión de Seguridad de Activos de Información

5.3.1. Objetivo

Identificar los activos de información de la Entidad y definir las responsabilidades de protección apropiadas.

5.3.2. Política

(a) Inventario de Activos de Información

La Oficina de Tecnologías de la Información y Datos Geofísicos del IGP, debe mantener un inventario de activos de información actualizada y revisada periódicamente, asimismo, dicho inventario debe contar con un propietario de activo de información. Esto será realizado a través del procedimiento Metodología de Gestión de Riesgos de Seguridad de la Información.

(b) Propietarios de Activos de Información

Los propietarios de activos de información son responsables de la gestión del activo de información durante todo su ciclo de vida, y deben:

1. Asegurarse que los activos son inventariados;
2. asegurarse que los activos son clasificados y protegidos adecuadamente;
3. definir y revisar periódicamente las restricciones de acceso y las clasificaciones de activos importantes, teniendo en cuenta las políticas aplicables de control de acceso;
4. garantizar el manejo adecuado cuando el activo es eliminado o destruido.

(c) Uso de Activos de información

(i) Los servidores deben usar los activos de información para los fines y objetivos del IGP, de acuerdo con los documentos normativos, la política, y procedimientos que se definan, y considerando los criterios de buen uso consignados en el **Anexo II Uso Aceptable de Activos de Información**.

(ii) Se deberá cumplir con los documentos normativos específicos, que cubren las prácticas requeridas para bienes y locales del IGP:


1. Directiva: N°5 2014 – Norma y Procedimiento para el Uso, cuidado y salida de bienes del IGP.
2. Directiva 006-2018 Control de ingresos y salidas en los locales del IGP

(iii) En el marco de las relaciones que el IGP debe cumplir con los requisitos legales, contractuales y normativos relativos al uso de activos de información, incluyendo los lineamientos de seguridad de la información que deben mantenerse alineados con la normatividad vigente.


(d) Devolución de Activos de información

(i) El IGP ha establecido el procedimiento para el retorno de los activos de información de la Entidad de los servidores que dejan de laborar en la Entidad a través de la Resolución de Gerencia General RGG-015-2020 Aprueba Directiva 003-2020-IGP/GG-OAD Disposiciones Para Regular el Procedimiento para Entrega y Recepción de Puesto de Servidores Civiles del IGP.

(e) Clasificación y manejo de la información

	LINEAMIENTO	Versión: 04
	LINEAMIENTO DE SEGURIDAD DE LA INFORMACIÓN	Código: LI 001-2020-IGP Sigla de Área: OTIDG

- (i) La clasificación y el manejo de la información se realiza en el marco del procedimiento de Gestión de Activos de Información de acuerdo a la “Guía para la clasificación y manejo de activos de información”.
 - (ii) Los propietarios de activos de información son responsables de clasificar la información que manejan en cada proceso o proyecto, de acuerdo a lo establecido en la Ley de Transparencia y Acceso a la Información Pública.
 - (iii) Los propietarios de los activos de información deberán etiquetar la información según la clasificación realizada. La información pública (pública e interna) no necesita una etiqueta. La información confidencial será etiquetada inicialmente en el documento que se utilice para realizar el inventario de activos de información y se aplicarán etiquetas en los metadatos asociados a la información.
- (f) Gestión de Medios Removibles:
- (i) El IGP no autoriza la utilización de medios removibles personales, para tal efecto pone a disposición los servicios de productividad suficientes.
 - (ii) El IGP solamente autoriza los medios removibles portátiles aprobados por la Oficina de Tecnologías de la Información y Datos Geofísicos.
 - (iii) Para el caso de los discos duros removibles y similares utilizados en computadoras de usuarios y servidores, la Oficina de Tecnologías de la Información y Datos Geofísicos del IGP, brinda la asistencia técnica que se requiera.
 - (iv) Para la eliminación de medios, se procede según el Anexo III Eliminación de Medios Removibles en caso corresponda. y se mantendrán los registros de las comunicaciones de las actividades realizadas.
 - (v) El servidor en el IGP, para proteger los medios que contienen información durante su transporte se debe seguir los siguientes criterios:
 1. Documentar una hoja de ruta (orden de salida de bienes).
 2. Se debe identificar en la hoja de ruta al destinatario (personal responsable de activo), transportista, origen, destino y el activo.
 3. De utilizarse proveedores para el transporte, se debe verificar que es un proveedor autorizado e identificarlo en la hoja de ruta, así mismo se debe lacrar el activo para evitar accesos no autorizados.
 4. De contener información confidencial se debe cumplir con la política de controles criptográficos.
 5. Utilizar vehículos y material de embalaje suficiente y de acuerdo con especificaciones de los fabricantes de hardware.
 6. No trasladar medios con soportes magnéticos (discos duros) en contacto con otros equipos que incluyen imanes potentes, como parlantes para eventos.

	LINEAMIENTO	Versión: 04
	LINEAMIENTO DE SEGURIDAD DE LA INFORMACIÓN	Código: LI 001-2020-IGP Sigla de Área: OTIDG


5.4. Política de Control de Accesos

5.4.1. Objetivos

- (a) Garantizar que la autorización de acceso a la información se realice de acuerdo con las atribuciones, funciones y/o tareas a desarrollar por el servidor.
- (b) Controlar los accesos a la información.
- (c) Prevenir accesos no autorizados a los sistemas de información y a los servicios de red.
- (d) Restringir el acceso a las instalaciones de procesamiento de información.


5.4.2. Política

- (a) Requerimientos para el control de accesos:
La Oficina de Tecnologías de la Información y Datos Geofísicos del IGP, establece que todos los accesos a los recursos de información deben basarse en la necesidad y rol del usuario, tomando en cuenta los siguientes aspectos:
 - (i) Los requerimientos de seguridad de cada una de las aplicaciones.
 - (ii) Identificación de toda la información relacionada a las aplicaciones y los riesgos a la que está expuesta.
 - (iii) Uso de perfiles de usuarios estandarizados definidos según roles.
 - (iv) Revisión periódica de los controles de acceso. Los propietarios de los activos revisan los derechos de acceso de los usuarios y deben notificar a la Oficina de Tecnologías de la Información y Datos Geofísicos sobre cualquier modificación necesaria.
 - (v) Revocación de los derechos de acceso.
- (b) Gestión de acceso del personal:
 - (i) Con el propósito de impedir accesos no autorizados a los recursos de información, La Oficina de Tecnologías de la Información y Datos Geofísicos del IGP, en coordinación con la Unidad de Logística, han establecido el control a través de la distribución de llaves, de acuerdo con listas visadas por las jefaturas de ambas unidades.
 - (ii) Todos los requerimientos de acceso a sistemas de información o accesos de red serán enviados a la Oficina de Tecnologías de la Información y Datos Geofísicos
 - (iii) Todo recurso que es gestionado con un sistema de acceso deberá contar con un formato de gestión de perfil de usuario.
 - (iv) Los responsables de las unidades orgánicas son los encargados de autorizar el acceso del servidor a su cargo, a los recursos de tecnologías de información y a las instalaciones de procesamiento de información, comunicando directamente a la Oficina de Tecnologías de la Información y Datos Geofísicos del IGP y a la Unidad de Logística, respectivamente.
 - (v) La Oficina de Tecnologías de la Información y Datos Geofísicos del IGP, debe asignar un usuario y contraseña que identifique única y


	LINEAMIENTO	Versión: 04
	LINEAMIENTO DE SEGURIDAD DE LA INFORMACIÓN	Código: LI 001-2020-IGP Sigla de Área: OTIDG

exclusivamente al servidor para el uso de los recursos informáticos, ya sea de forma temporal o permanente.

- (vi) La Oficina de Tecnologías de la Información y Datos Geofísicos del IGP, configura la red de manera que no se compartan identificadores entre diferentes usuarios ni pueda permitirse la duplicidad de sesiones de usuarios.
- (vii) La Oficina de Tecnologías de la Información y Datos Geofísicos del IGP, gestiona la asignación y habilitación o revocación de usuarios del Servicio de Directorio.
- (viii) Para los servicios no vinculados al Servicio de Directorio, se registran y cancelan usuarios a través de los paneles de control específicos de administración.
- (ix) Es posible asignar accesos a terceros, en este caso se asignan cuentas de usuario genéricas y a solicitud del responsable de la unidad orgánica solicitante.
- (x) Para usuarios privilegiados (administradores), se gestionan mediante el formato *solicitud de acceso* por el propietario del activo de información (sistemas de información).
- (c) Gestión de usuarios / contraseñas
 - (i) Los usuarios/contraseñas gestionadas mediante el servicio de directorio se proporcionarán por primera vez al usuario según el siguiente criterio:
 1. En el caso de servidores, la URH remite la lista oficial para el alta de usuarios, tras lo cual OTIDG se contacta con los nuevos usuarios por medio de llamadas telefónicas para proporcionarles sus credenciales.
 2. En el caso de terceros, el área responsable del servicio debe solicitar a OTIDG la creación de las cuentas genéricas necesarias para la prestación, tras lo cual OTIDG envía las credenciales al área responsable por correo electrónico, las cuales son reenviadas al tercero.
 - (ii) Los usuarios/contraseñas de sistemas y servicios no vinculados al servicio de directorio deben ser solicitados a OTIDG, mediante el uso del procedimiento Atención TIC y eventos e incidentes de SI. En este caso las credenciales se entregan al solicitante a través del correo electrónico institucional.
 - (iii) Los usuarios/contraseñas de los repositorios de desarrollo de soluciones informáticas son gestionados de manera centralizada por el Coordinador de Ingeniería de Software, quien genera cuentas vinculadas a usuarios institucionales a través de nombres de usuario coincidentes con correos electrónicos asignados y a través de un repositorio local. Las credenciales se entregan a los usuarios autorizados a través del correo electrónico.
 - (iv) Para el caso de las cuentas gestionadas por el servicio de directorio, los usuarios están obligados a cambiar sus contraseñas de acceso inicial en un plazo no mayor a un mes, para esto se dispone de un servicio web con certificados digitales, desde donde los usuarios pueden cambiar sus contraseñas.
 - (v) Las contraseñas almacenadas en bases de datos deben ser cifradas con un patrón criptográfico de mínimo 256 bits.


	LINEAMIENTO	Versión: 04
	LINEAMIENTO DE SEGURIDAD DE LA INFORMACIÓN	Código: LI 001-2020-IGP Sigla de Área: OTIDG

- (vi) Cada servidor es responsable de la confidencialidad de la contraseña asignada, y de las consecuencias por las acciones que, mediante su uso, terceras personas pueden realizar.
- (vii) Las contraseñas son estrictamente personales e intransferibles y el servidor es responsable de mantener su confidencialidad.
- (viii) Para el caso de servicios o equipos con administración compartida, el proveedor entregará las credenciales a través de informes de instalación dirigidos a la jefatura de OTIDG.
- (ix) Las reglas de conformación de contraseñas deben estar automatizadas en todos los sistemas donde esto es viable, de modo que los sistemas rechacen contraseñas débiles. El estándar de conformación de contraseñas se encuentra en el Anexo IV Estándar de Contraseñas
- (d) Control de acceso a las redes informáticas:
 - (i) El acceso a los recursos de red, internos y externos debe ser controlado por La Oficina de Tecnologías de la Información y Datos Geofísicos del IGP, de manera que el servidor no comprometa la seguridad de los activos de información.
 - (ii) Para la seguridad en las redes informáticas, se deben tener en cuenta los siguientes aspectos:
 1. Lineamientos de uso de la red.
 2. Segmentación de redes. Se utilizará la segmentación de redes, gestionada por el firewall. Cada usuario ingresa al segmento que le ha sido asignado. De necesitar ingresar a un segmento distinto, debe solicitarlo a la Oficina de Tecnologías de la Información y Datos Geofísicos, previo Vo Bo de su jefe inmediato. La justificación de la necesidad debe incluirse en el requerimiento. La Oficina de Tecnologías de la Información y Datos Geofísicos del IGP puede denegar el requerimiento si la justificación no guarda coherencia con el acceso solicitado.
 3. Control de conexiones a redes en base a la política.
 4. Controles de enrutamiento de redes.
- (e) Control de acceso a los sistemas operativos:
 - (i) El acceso a los sistemas operativos de las estaciones de trabajo del IGP, debe ser debidamente controlado por la Oficina de Tecnologías de la Información y Datos Geofísicos del IGP, a fin de evitar accesos no autorizados a recursos o información.
 - (ii) Dentro de los aspectos que deben ser tomados en consideración para definir los controles, se incluyen:
 1. Identificación automática de estación de trabajo
 2. Inicio de sesión seguro.
 3. Identificación y autenticación de usuarios.
 4. Sistema de gestión de contraseñas.
 5. Restricción del uso de herramientas utilitarias del sistema operativo con capacidades de eludir y/o sobrescribir los controles de seguridad.
- (f) Control de acceso a las aplicaciones:

	LINEAMIENTO	Versión: 04
	LINEAMIENTO DE SEGURIDAD DE LA INFORMACIÓN	Código: LI 001-2020-IGP Sigla de Área: OTIDG

- (i) La Oficina de Tecnologías de la Información y Datos Geofísicos del IGP, controla los accesos a la información y a las aplicaciones del servicio de productividad, restringiendo para uso exclusivo del personal debidamente autorizado; asimismo, revisar periódicamente los accesos concedidos, revocando los derechos cuya vigencia de autorización haya caducado. Para esto, se cuenta con:
 - 1. Administración compartida con el proveedor del servicio para asesoría de opciones avanzadas.
 - 2. Una cuenta de correo en el dominio se asigna como administrador
 - 3. Documento firmado entre el IGP y el proveedor gestionado al inicio del servicio, con las cuentas con acceso y el tipo de acceso. Cualquier modificación es consultada a quien firmó el acuerdo.
- (ii) Se deben aislar los sistemas identificados con información sensible, asignándoles un entorno de procesamiento dedicado, creado a partir de métodos físicos o lógicos.
- (g) Conexiones externas:

En cualquier caso, para el acceso remoto (todo acceso a la información del IGP fuera del centro de trabajo) se debe utilizar la tecnología y acceso seguro (SSL-VPN) y su uso debe ser autorizado solo en caso de ser necesario por el jefe del órgano o unidad orgánica y La Oficina de Tecnologías de la Información y Datos Geofísicos, con el conocimiento del Oficial de Seguridad de la información.

	LINEAMIENTO	Versión: 04
	LINEAMIENTO DE SEGURIDAD DE LA INFORMACIÓN	Código: LI 001-2020-IGP Sigla de Área: OTIDG

5.5. Política de Seguridad Física y del Entorno

5.5.1. Objetivo


Tomar las medidas necesarias para evitar el acceso físico no autorizado, los daños e interferencia a la información de la Entidad y a los recursos de tratamiento de la información.

5.5.2. Política


- (a) Los perímetros de seguridad física están establecidos en planos de arquitectura. Se ha determinado perímetros externos con paredes de material noble. Asimismo, se han marcado las áreas internas sensibles:
 - (i) Centros de Datos
 - (ii) CENSIS
 - (iii) Salas de UPS
 - (iv) Antena parabólica
 - (v) Zona de grupos electrógenos
- (b) El servidor del IGP que atiende a personas externas a la Entidad (incluyendo suministradores) debe asegurar que los datos de todas las visitas de personas externas a la Entidad quedan anotados en el registro de visitas. En relación a esto, se debe revisar la Directiva Control de ingresos y salidas en los locales del IGP.
- (c) La Oficina de Tecnologías de la Información y Datos Geofísicos del IGP, supervisa que se controlen de manera estricta las llaves de los Centros de Datos videovigilancia en puntos clave que incluyen las áreas sensibles.
- (d) La Oficina de Tecnologías de la Información y Datos Geofísicos del IGP, establece una clasificación de las áreas para definir el nivel de seguridad de las mismas, las cuales se describen a continuación:

ÁREA	DESCRIPCIÓN
Restringida	Son zonas seguras donde la información que se genera transmite, trata o almacena es crítica para la entidad. Los accesos a estos despachos son controlados.
Común	Son zonas de uso común para el servidor del IGP.
Pública	Son zonas que son de utilización pública y de recepción de personas externas a la entidad.

- (e) Toda persona externa al IGP puede acceder a las áreas definidas como restringidas, siempre que cuente con la autorización respectiva del jefe del órgano o unidad orgánica y debe estar siempre acompañado por un servidor de la Entidad.
- (f) El servidor del IGP debe portar en todo momento su fotocheck para su debida identificación.

	LINEAMIENTO	Versión: 04
	LINEAMIENTO DE SEGURIDAD DE LA INFORMACIÓN	Código: LI 001-2020-IGP Sigla de Área: OTIDG

- (g) Los visitantes que ingresan a las instalaciones del IGP deben portar en todo momento su pase de visita.
- (h) El personal de IGP debe seguir el procedimiento establecido en la Norma y Procedimiento para el Uso, cuidado y salida de bienes del IGP establecido en la entidad para el movimiento de activos como computadoras.
- (i) Todos los equipos de cómputo que ingresan al IGP deben ser previamente registrados por el personal de seguridad responsable.
- (j) El IGP a través de los Órganos y Unidades Orgánicas de acuerdo a su responsabilidad debe de implementar medidas de protección contra amenazas externas y ambientales, dichas medidas de protección, debe incluir:
 - (i) Controles de acceso y seguridad física
 - (ii) Detectores de humo.
 - (iii) Extintores
 - (iv) Sistema de alimentación ininterrumpida (UPS)
 - (v) Sistema de puesta a Tierra
 - (vi) Grupo Electrónico
- (k) La Oficina de Tecnologías de la Información y Datos Geofísicos del IGP, debe proteger los equipos de Tecnologías de la información de fallas por falta de suministro de energía y otras anomalías eléctricas.
- (l) La Oficina de Tecnologías de la Información y Datos Geofísicos del IGP, debe proteger el cableado de la red de comunicaciones y suministro de energía para evitar interceptación o daño.
- (m) El cableado de suministro de energía eléctrica y telecomunicaciones en las Zonas de tratamiento de información debe contar con un sistema de pozo a tierra, el que debe ser revisado periódicamente para garantizar su adecuado funcionamiento.
- (n) La Oficina de Tecnologías de la Información y Datos Geofísicos del IGP, debe mantener programas de mantenimiento de los equipos de Tecnologías de información
- (o) Servicios Generales debe mantener programas de mantenimiento de los sistemas de acondicionamiento de temperatura, humedad, sistemas de energía ininterrumpida (UPS) y sistemas de detección y extinción de fuego, a fin de garantizar la continuidad de los servicios.
- (p) La Oficina de Tecnologías de la Información y Datos Geofísicos del IGP, debe implementar una Política de Escritorio Limpio y Pantalla Limpia, a fin de evitar el acceso no autorizado y el uso indebido de la información.

	LINEAMIENTO	Versión: 04
	LINEAMIENTO DE SEGURIDAD DE LA INFORMACIÓN	Código: LI 001-2020-IGP Sigla de Área: OTIDG


5.6. Política de Seguridad de las Operaciones

5.6.1. Objetivo

Asegurar que las operaciones de instalaciones de procesamiento de la información sean correctas y seguras.


5.6.2. Política

- (a) **Procedimientos Operativos Documentados:**
La Oficina de Tecnologías de la Información y Datos Geofísicos del IGP, debe documentar procedimientos operativos, estableciendo las responsabilidades y los recursos utilizados para su ejecución eficiente, asimismo, estos deberán estar a disposición de los servidores autorizados.
- (b) **Gestión de Cambios:**
 - (i) La Oficina de Tecnologías de la Información y Datos Geofísicos del IGP, debe mantener un registro de control de cambios de los sistemas, equipos de comunicación, bases de datos, equipos de cómputo y perfiles de acceso, a través de la implementación de acciones y procedimientos orientados a asegurar que todo cambio siga un proceso planificado que incluya responsabilidades y canales de comunicación, identificación de los recursos comprometidos, pruebas de comprobación y estrés, controles de seguridad; reversión en caso de fallas y análisis de impacto.
 - (ii) Todos los cambios deben ser solicitados a La Oficina de Tecnologías de la Información y Datos Geofísicos del IGP, por el propietario de la información, y se llevará un registro sobre cada solicitud de cambio. En caso existiera algún problema con el cambio realizado, se revertirá al estado anterior al cambio.
- (c) **Gestión de la Capacidad:**
La Oficina de Tecnologías de la Información y Datos Geofísicos del IGP, debe garantizar la capacidad de los recursos a fin de asegurar el desempeño requerido de los Sistemas de información.
- (d) **Separación de Entornos:**
 - (i) La Oficina de Tecnologías de la Información y Datos Geofísicos del IGP, debe separar entornos de desarrollo, pruebas y producción con el fin de prevenir riesgos de acceso no autorizado o cambios al entorno operativo.
 - (ii) La Oficina de Tecnologías de la Información y Datos Geofísicos del IGP, debe venir y documentar procedimientos para pases de desarrollo a producción, asimismo, el entorno de pruebas debe ser en lo posible, igual al ambiente de producción en lo referido a recursos de Tecnologías de información.
- (e) **Protección contra Software Malicioso**
 - (i) La Oficina de Tecnologías de la Información y Datos Geofísicos del IGP, debe adoptar las medidas necesarias para la prevención, detección y eliminación de código malicioso (malware) a nivel de servidores de red, computadoras portátiles, estaciones de trabajo, tabletas, teléfonos inteligentes, etc.
 - (ii) La Oficina General de Tecnologías de Información del IGP, debe asegurar que todas las estaciones de trabajo estén protegidas con el antivirus


	LINEAMIENTO	Versión: 04
	LINEAMIENTO DE SEGURIDAD DE LA INFORMACIÓN	Código: LI 001-2020-IGP Sigla de Área: OTIDG

corporativo y que este se encuentre actualizado. Asimismo, debe garantizar que el sistema operativo y los aplicativos de oficina cuenten con las últimas actualizaciones de seguridad (parches).

- (iii) La Oficina de Tecnologías de la Información y Datos Geofísicos del IGP, es responsable de la renovación de licencias de software, y debe definir su cronograma de renovación, para evitar que se produzca incumplimiento de uso ilegal de software.
- (iv) El Software utilizado por el IGP debe ser autorizado en forma expresa por La Oficina de Tecnologías de la Información y Datos Geofísicos del IGP.
- (v) El personal de soporte técnico de La Oficina de Tecnologías de la Información y Datos Geofísicos del IGP, como medida de prevención, si detecta que alguna estación de trabajo o computadora portátil se encuentra infectada con algún tipo de malware, debe aislarla inmediatamente, desconectandola de la red corporativa.
- (f) Respaldo de Información:
 - (i) La Oficina de Tecnologías de la Información y Datos Geofísicos del IGP, debe establecer procedimientos rutinarios para el respaldo de la información, de acuerdo con su criticidad, realizando copias de seguridad y pruebas de recuperación, conforme a un cronograma definido.
 - (ii) La Oficina de Tecnologías de la Información y Datos Geofísicos del IGP, debe resguardar las copias de seguridad en un ambiente distinto al del origen de la información (es decir, en un local distinto), que reúna las condiciones adecuadas de acondicionamiento, temperatura y humedad.
 - (iii) La Oficina de Tecnologías de la Información y Datos Geofísicos del IGP, debe asegurar que los equipos y los medios de respaldo cuentan con un programa de mantenimiento preventivo y correctivo para asegurar su correcto funcionamiento.
 - (iv) La Oficina de Tecnologías de la Información y Datos Geofísicos del IGP, debe estimar anticipadamente la cantidad necesaria de medios magnéticos u otros requeridos para realizar las copias de respaldo y, en caso de no contar con ello, solicitar su oportuna adquisición.
 - (v) La Oficina de Tecnologías de la Información y Datos Geofísicos del IGP, debe mantener el registro actualizado de las operaciones de gestión de respaldo y recuperación, así como de las fallas que pudieran presentarse y las soluciones realizadas, a través del personal de soporte técnico.
 - (vi) La Oficina de Tecnologías de la Información y Datos Geofísicos del IGP, debe de realizar pruebas de restauración a las copias de seguridad con el fin de asegurar que se pueda obtener correctamente la información almacenada al momento de ser necesaria.
 - (vii) La Oficina de Tecnologías de la Información y Datos Geofísicos del IGP, debe revisar periódicamente la vigencia tecnológica de los equipos y software utilizados para el respaldo y recuperación de la información.
- (g) Registro y Monitoreo:
 - (i) Todos los servicios informáticos se encuentran sujetos a monitoreo por parte de La Oficina de Tecnologías de la Información y Datos Geofísicos del IGP.

	LINEAMIENTO	Versión: 04
	LINEAMIENTO DE SEGURIDAD DE LA INFORMACIÓN	Código: LI 001-2020-IGP Sigla de Área: OTIDG

- (ii) La Oficina de Tecnologías de la Información y Datos Geofísicos del IGP, debe generar registros de auditoría sobre el uso de los recursos de Tecnologías de información.
- (iii) Las actividades de los operadores y administradores de los sistemas de La Oficina de Tecnologías de la Información y Datos Geofísicos del IGP, deben ser monitoreadas, registradas, verificadas regularmente y periódicamente por La Oficina de Tecnologías de la Información y Datos Geofísicos del IGP.
- (iv) La Oficina de Tecnologías de la Información y Datos Geofísicos del IGP, debe contar con registro de fallas en los sistemas de información para seguimiento, registros de auditoría y monitoreo pertinente.
- (v) Cada servidor del IGP es responsable de todas las actividades realizadas a través de sus cuentas de acceso de red, correo electrónico, sistemas de información asociados y sistemas.
- (h) Sincronización de Reloj:
La Oficina de Tecnologías de la Información y Datos Geofísicos del IGP, debe mantener sincronizado los relojes en los Sistemas de información con una fuente exacta que establece la "Hora Oficial de la República del Perú", a fin de garantizar la exactitud de los registros.
- (i) Control de Software Operacional:
La Oficina de Tecnologías de la Información y Datos Geofísicos del IGP, debe implementar mecanismos de restricción para la instalación de software en los equipos de cómputo por parte de los usuarios no autorizados.
- (j) Controles de Auditoría de los Sistemas de Información:
 - (i) Todos los servicios informáticos se encuentran sujetos a monitoreo por parte de La Oficina de Tecnologías de la Información y Datos Geofísicos.
 - (ii) La Oficina de Tecnologías de la Información y Datos Geofísicos del IGP, debe generar registros de auditoría sobre el uso de los recursos de Tecnologías de información.

	LINEAMIENTO	Versión: 04
	LINEAMIENTO DE SEGURIDAD DE LA INFORMACIÓN	Código: LI 001-2020-IGP Sigla de Área: OTIDG


5.7. Política de Seguridad de las Comunicaciones

5.7.1. Objetivo

- (a) Asegurar la protección de la información en las redes y sus instalaciones de procesamiento de la información de apoyo.
- (b) Proteger la información de las redes y la infraestructura que la soporta.
- (c) Monitorear las actividades de procesamiento de información no autorizadas.

5.7.2. Política


- (a) La Oficina de Tecnologías de la Información y Datos Geofísicos del IGP, debe implementar mecanismos de control y procedimientos necesarios para proveer la disponibilidad de las redes de datos y de los servicios que dependen de ellas; asimismo, vela por que se cuente con controles de seguridad que protejan la integridad y la confidencialidad de la información que se transporta a través de dichas redes de datos.
- (b) La Oficina de Tecnologías de la Información y Datos Geofísicos del IGP, debe realizar la segregación de redes, a fin de garantizar su debida protección.
- (c) Seguridad de Correo Electrónico
 - (i) La Oficina de Tecnologías de la Información y Datos Geofísicos del IGP, puede efectuar la deshabilitación de la cuenta de correo electrónico institucional por algún uso indebido que transgrede lo establecido en el presente documento.
 - (ii) Cada servidor es responsable por la información que se transmita desde la cuenta de correo electrónico que le haya asignado la Entidad.
 - (iii) En caso el servidor reciba mensajes con asuntos sospechosos y/o de origen desconocido, estos no deben ser abiertos y deben comunicarse inmediatamente a la Oficina de Tecnologías de información del IGP, según corresponda, así como al Oficial de Seguridad de la información para los fines correspondientes y luego deben ser eliminados.
 - (iv) El servidor debe usar firmas estandarizadas, de conformidad con el modelo establecido por la Unidad Funcional de Comunicaciones y OTIDG.
 - (v) El envío de mensajes masivos de correo electrónico dentro de la Entidad está permitido solo para el personal o dependencias autorizados por la Alta Dirección del IGP.

	LINEAMIENTO	Versión: 04
	LINEAMIENTO DE SEGURIDAD DE LA INFORMACIÓN	Código: LI 001-2020-IGP Sigla de Área: OTIDG

(d) Acuerdo de Confidencialidad

La Oficina de Tecnologías de la Información y Datos Geofísicos del IGP, asegura la protección de la información en el momento de ser transferida o intercambiada y establece los procedimientos y controles necesarios para el intercambio de información; asimismo, se establecen Acuerdos de Confidencialidad y/o de intercambio de información con terceras partes y/o con quienes corresponda.

La Oficina de Tecnologías de la Información y Datos Geofísicos del IGP, vela por el uso de Tecnologías informáticas y de telecomunicaciones para llevar a cabo el intercambio de información; de acuerdo a lo establecido en los acuerdos que contraiga.

	LINEAMIENTO	Versión: 04
	LINEAMIENTO DE SEGURIDAD DE LA INFORMACIÓN	Código: LI 001-2020-IGP Sigla de Área: OTIDG


5.8. Política de Adquisición, Desarrollo y Mantenimiento de Sistemas

5.8.1. Objetivos

- (a) Asegurar que los sistemas cumplan con los requisitos de seguridad de la Entidad.
- (b) Evitar pérdidas, modificaciones o mal uso de la información que se encuentra dentro de los sistemas.
- (c) Proteger la confidencialidad, autenticidad e integridad de los sistemas del IGP.

5.8.2. Política

- (a) Metodología para la adquisición, desarrollo y mantenimiento de los sistemas:
 - (i) La Oficina de Tecnologías de la Información y Datos Geofísicos del IGP, debe aprobar un procedimiento para la adquisición, desarrollo y mantenimiento de los sistemas.
 - (ii) Todo desarrollo y/o mantenimiento de sistemas debe ser documentado, con la finalidad de que personas no familiarizadas con ellas en el IGP, ejecuten las actividades con facilidad.
- (b) Requisitos de seguridad de los sistemas:
 - (i) La Oficina de Tecnologías de la Información y Datos Geofísicos del IGP, debe definir un procedimiento que incluya controles de seguridad durante las etapas de análisis y diseño de los sistemas.
 - (ii) Todo sistema desarrollado por los servidores de La Oficina de Tecnologías de la Información y Datos Geofísicos del IGP o por terceros, debe satisfacer los requisitos de seguridad definidos para el desarrollo y mantenimiento de los sistemas. En el caso de los terceros, el desarrollo de los sistemas debe constar en el respectivo contrato de prestación de servicios.
 - (iii) El servidor debe cumplir los controles, estándares y metodologías referidas al desarrollo de los sistemas seguros que se hayan implementado.
 - (iv) La Oficina de Tecnologías de la Información y Datos Geofísicos del IGP, debe verificar que los acuerdos sobre materia informática a suscribir con terceros incluyan cláusulas relativas a la cesión de derechos y confidencialidad de la información, para el resguardo de la propiedad intelectual del IGP.
 - (v) Los acuerdos que involucran el acceso, procesamiento, comunicación o manejo de terceros de las instalaciones de procesamiento de información, deben cubrir los requisitos de seguridad necesarios.
 - (vi) Todos los sistemas desarrollados por los servidores son de propiedad del IGP.
- (c) Procesamiento correcto de los sistemas:
 - (i) La Oficina de Tecnologías de la Información y Datos Geofísicos del IGP, debe implementar controles de seguridad apropiados en los sistemas utilizados por el IGP, para validar los datos de entrada, el procesamiento interno y los datos de salida.
 - (ii) La Oficina de Tecnologías de la Información y Datos Geofísicos del IGP, debe identificar los requerimientos para asegurar la autenticidad y la integridad de los mensajes en los sistemas, debiendo definirse e implementar los controles apropiados.

	LINEAMIENTO	Versión: 04
	LINEAMIENTO DE SEGURIDAD DE LA INFORMACIÓN	Código: LI 001-2020-IGP Sigla de Área: OTIDG

(d) Seguridad de los archivos de los sistemas:

La Oficina de Tecnologías de la Información y Datos Geofísicos del IGP, deben implementar controles sobre lo siguiente:

- (i) Control de los sistemas en Producción: Comprende la formulación y puesta en práctica de procedimientos orientados a controlar la instalación de los sistemas en producción.
- (ii) Protección de Datos de Prueba: Los datos de prueba de los sistemas deben ser cuidadosamente seleccionados, protegidos y controlados.

(e) Control de acceso al Código Fuente de los sistemas:

La Oficina de Tecnologías de la Información y Datos Geofísicos del IGP controla el acceso al código fuente de las aplicaciones que desarrolla el IGP a través de la asignación de cuentas institucionales para los repositorios utilizados. Estos mantienen trazabilidad y registro de los cambios y salidas de código fuente.

(f) Uso de controles criptográficos:

La Oficina de Tecnologías de la Información y Datos Geofísicos del IGP, debe implementar el uso de controles para cifrar la información y proteger la confidencialidad, autenticidad e integridad de la misma. Se utilizarán certificados digitales de 2048 bits. Las claves criptográficas se gestionan a través del registro de fechas de activación, renovación y desactivación.

(g) Seguridad en los procesos de desarrollo y pase a producción:

- (i) Procedimiento para el desarrollo de los sistemas: Todo el desarrollo y mantenimiento de los sistemas en el IGP deben ser realizados conforme a los procedimientos establecidos, debiendo considerarse la NTP ISO/IEC 12207 y otros estándares pertinentes.


(ii) Procedimiento para pase a producción: `

1. Los servidores encargados del desarrollo y mantenimiento de los sistemas, así como los terceros, no tendrán acceso a los datos de producción.
2. Los ambientes de desarrollo y producción deben ser configurados en servidores diferentes, limitando el acceso solo al personal autorizado.
3. El pase a producción debe ser realizado exclusivamente por la persona autorizada por La Oficina de Tecnologías de la Información y Datos Geofísicos del IGP, quien lleva un control de los pases efectuados y/o actualizaciones de los sistemas en un registro o bitácora.
4. Todo desarrollo, antes de su pase a producción, debe ser revisado por La Oficina de Tecnologías de la Información y Datos Geofísicos del IGP, para asegurar que se cumplan los estándares establecidos.


(h) Control de cambios de los sistemas:

- (i) El control, registro y monitoreo de los cambios de los sistemas del IGP debe ser supervisado y registrado por La Oficina de Tecnologías de la Información y Datos Geofísicos del IGP.
- (ii) Todo acceso a la librería de los programas fuente debe ser controlado por La Oficina de Tecnologías de la Información y Datos Geofísicos del IGP, a fin de evitar accesos y/o cambios no autorizados.

(i) Gestión de vulnerabilidades técnicas:

	LINEAMIENTO	Versión: 04
	LINEAMIENTO DE SEGURIDAD DE LA INFORMACIÓN	Código: LI 001-2020-IGP Sigla de Área: OTIDG

- (i) La Oficina de Tecnologías de la Información y Datos Geofísicos del IGP, debe programar la realización de pruebas de comprobación técnica a cargo de especialistas para verificar que se han implementado correctamente los controles de seguridad definidos para el hardware y software.
- (ii) Identificadas las vulnerabilidades técnicas, La Oficina de Tecnologías de la Información y Datos Geofísicos del IGP, debe determinar los riesgos asociados e implementar los controles necesarios para mitigarlos. Los sistemas críticos y en alto riesgo deben ser tratados primero.
- (iii) Para los sistemas que requieren una actualización de seguridad (parches), La Oficina de Tecnologías de la Información y Datos Geofísicos del IGP, debe probar y evaluar su efectividad en un ambiente de pruebas; asimismo, se deben considerar los riesgos asociados a su aplicación y, en todas las cosas, se deben cumplir los controles establecidos para la gestión de cambios.

	LINEAMIENTO	Versión: 04
	LINEAMIENTO DE SEGURIDAD DE LA INFORMACIÓN	Código: LI 001-2020-IGP Sigla de Área: OTIDG

5.9. Política de control criptográfico

5.9.1. Objetivo

Definir el uso adecuado y eficaz de los controles criptográficos para proteger la confidencialidad, integridad y disponibilidad de la información en el IGP.

5.9.2. Política


a) Uso de controles criptográficos:

El IGP debe emplear controles criptográficos,

- i) Para proteger las claves de acceso a sistemas, datos y servicios.
- ii) Para proteger la transmisión de información sensible, confidencial o reservada de acuerdo a la clasificación de la información.
- iii) Para proteger la información en dispositivos extraíbles o móviles, toda vez que posean información confidencial.
- iv) Para el resguardo de la información que resulte de la evaluación de riesgos.

b) Gestión de claves

- i) Solo se deben utilizar algoritmos criptográficos confiables y válidos.
- ii) El acceso a las claves privadas del cifrado, sólo debe estar permitido al propietario del activo y personas autorizadas.
- iii) Todas las claves criptográficas privadas, deben estar protegidas contra modificación, divulgación y eliminación por un acceso no autorizado.

	LINEAMIENTO	Versión: 04
	LINEAMIENTO DE SEGURIDAD DE LA INFORMACIÓN	Código: LI 001-2020-IGP Sigla de Área: OTIDG


5.10. Política de Relación con Proveedores

5.10.1. Objetivos

Garantizar la protección de los activos de información del IGP, que son accesibles por los Proveedores.


5.10.2. Política

- (a) Todo proveedor que brinde servicios a IGP, debe suscribir un acuerdo de confidencialidad, la misma que será parte del contrato de prestación de servicios como anexo.
- (b) Los proveedores sólo podrán desarrollar para IGP, aquellas actividades cubiertas bajo el correspondiente contrato u orden de prestación de servicios.
- (c) El proveedor debe proporcionar los datos completos de la persona de contacto, quien se encarga de recibir todo tipo de directivas de seguridad de la información.
- (d) El proveedor proporciona mensualmente, mientras dure la vigencia del contrato, la relación de personas, perfiles, funciones y responsabilidades asociadas al servicio provisto, e informa puntualmente de cualquier cambio (alta, baja, sustitución o cambio de funciones o responsabilidades) que se produzca en dicha relación.
- (e) Todo proveedor de servicios debe velar porque su personal que presta los servicios directamente a IGP, cumpla con las políticas de seguridad de la información recogidas en el presente documento. En caso de incumplimiento, IGP se reserva el derecho de solicitar al proveedor el cambio de personal, sin perjuicio del derecho de IGP, de resolver el contrato de prestación de servicios en los términos establecidos en el contrato.
- (f) Cualquier tipo de intercambio de información que se produzca entre IGP y el proveedor se debe entender que ha sido realizado dentro del marco establecido por el contrato u orden de prestación de servicios, de modo que dicha información tendrá el carácter de confidencial y no podrá ser utilizada en ningún caso fuera de dicho marco, ni para fines diferentes a los asociados al contrato.
- (g) Todo proveedor que tenga acceso a la información del IGP, en ejecución de un contrato u orden de prestación de servicios, debe considerar que dicha información, es confidencial y está sujeto a la Ley de Protección de Datos Personales.
- (h) Ningún proveedor puede utilizar la información del IGP para beneficio propio o de terceros. La información a la que tenga acceso el proveedor únicamente puede ser utilizada para los fines específicamente indicados en el contrato u orden de prestación de servicios, Toda información proporcionada por el IGP, sigue siendo de propiedad de esta última.
- (i) El proveedor y su personal únicamente puede utilizar la información y activos tecnológicos autorizados por el IGP para el desarrollo de los servicios contratados.
- (j) La distribución de la información ya sea en formato digital o papel, se realiza mediante los recursos determinados en el contrato de prestación de servicios y para la finalidad exclusiva de facilitar las funciones asociadas a dicho contrato.

	LINEAMIENTO	Versión: 04
	LINEAMIENTO DE SEGURIDAD DE LA INFORMACIÓN	Código: LI 001-2020-IGP Sigla de Área: OTIDG

El IGP, se reserva, en función del riesgo identificado, la implementación de medidas de control, registro y auditoría sobre los recursos de difusión.

- (k) Los recursos que el IGP pone a disposición del proveedor, independientemente del tipo que sean, (informáticos, datos, software, redes, sistemas de comunicación, etc.) están exclusivamente destinados para cumplir con las obligaciones y propósito para los que fueron proporcionados. IGP se reserva el derecho de implementar mecanismos de control y auditoría que verifiquen el uso apropiado de estos recursos.
- (l) El proveedor debe notificar a La Oficina de Tecnologías de la Información y Datos Geofísicos del IGP, cualquier incidencia que se detecte y que afecte o pueda afectar a la seguridad de la información de la Entidad.

	LINEAMIENTO	Versión: 04
	LINEAMIENTO DE SEGURIDAD DE LA INFORMACIÓN	Código: LI 001-2020-IGP Sigla de Área: OTIDG


5.11. Política de Gestión de Incidentes de Seguridad de la información

5.11.1. Objetivos

Asegurar que los incidentes de seguridad de la información sean comunicados oportunamente a las instancias correspondientes, con la finalidad de adoptar acciones preventivas y correctivas que correspondan.

5.11.2. Política

- (a) Los incidentes relativos a la seguridad de la información deben ser comunicados a La Oficina de Tecnologías de la Información y Datos Geofísicos del IGP y al Oficial de Seguridad de la Información, conforme al procedimiento que se establezca para tal efecto.
- (b) El servidor del IGP debe conocer el procedimiento de gestión de incidentes de seguridad de la información, e informar de su ocurrencia tan pronto tome conocimiento de ellos.
- (c) Cualquier servidor del IGP debe comunicar al Oficial de Seguridad de la información del IGP, sugerencias, debilidades, vulnerabilidades y/o situaciones de riesgo que puede tener relación con la seguridad de la información y las directrices contempladas en las presentes políticas de las que tenga conocimiento.
- (d) El servidor del IGP debe conocer su responsabilidad respecto a la comunicación de los incidentes de seguridad que tome conocimiento, debiendo ser notificado de los resultados una vez que el incidente haya sido resuelto.
- (e) Toda persona externa a la institución que ingresa al IGP, debe ser notificado por los agentes de seguridad, de manera verbal y a través de las papeletas de visita, el requisito de notificar a OTIDG por los canales que corresponda, cualquier debilidad detectada en la Seguridad de la Información. En el caso de que se trate de proveedores, se notificará también en la orden de compra O/C u O/S.
- (f) Reportados los incidentes de seguridad de la información a La Oficina de Tecnologías de la Información y Datos Geofísicos del IGP, y al Oficial de Seguridad de la Información, debe proceder a su exhaustivo análisis por parte del servidor que designe la referida oficina o dependencia del programa, a efectos de adoptar las acciones que correspondan.
- (g) Los incidentes de seguridad serán evaluados por el Comité de Gestión de Seguridad de la información del IGP, a efectos de proponer las acciones preventivas que correspondan, para lo sucesivo.
- (h) Periódicamente, La Oficina de Tecnologías de la Información y Datos Geofísicos del IGP, debe analizar las actividades realizadas y estudiar posibles mejoras o cambios que puedan proponerse al Comité de Gestión de Seguridad de la información para prevenir la ocurrencia de futuros incidentes de Seguridad de la información.

	LINEAMIENTO	Versión: 04
	LINEAMIENTO DE SEGURIDAD DE LA INFORMACIÓN	Código: LI 001-2020-IGP Sigla de Área: OTIDG


5.12. Política de Continuidad de la Seguridad de la información

5.12.1. Objetivos

- (a) Preservar la seguridad de la información durante las fases de activación, de desarrollo de procesos, procedimientos y planes para la continuidad de negocio y de vuelta a la normalidad.
- (b) Garantizar la disponibilidad de los recursos de tratamiento de la información.

5.12.2. Política

- (a) La Oficina de Tecnologías de la Información y Datos Geofísicos del IGP, debe incluir la continuidad de la seguridad de la información dentro del proceso de gestión de continuidad operativa.
- (b) La Oficina de Tecnologías de la Información y Datos Geofísicos del IGP, debe verificar los controles de continuidad de seguridad de la información que se han implementado regularmente para asegurar que sean válidos y efectivos.
- (c) La Oficina de Tecnologías de la Información y Datos Geofísicos del IGP, debe asegurar la existencia de recursos redundantes para el tratamiento de la información a fin de cumplir con los requisitos de disponibilidad.
- (d) La Oficina de Tecnologías de la Información y Datos Geofísicos del IGP, debe realizar las pruebas de la funcionalidad de los procesos, procedimientos y controles de continuidad de la seguridad de la información para garantizar que se encuentran conforme a los objetivos de continuidad de la seguridad de la información, estas pruebas deben quedar documentadas.

	LINEAMIENTO	Versión: 04
	LINEAMIENTO DE SEGURIDAD DE LA INFORMACIÓN	Código: LI 001-2020-IGP Sigla de Área: OTIDG


5.13. Política de Cumplimiento y de Protección y Privacidad de Datos Personales

5.13.1. Objetivos

- (a) Prevenir incumplimientos de las obligaciones legales, estatutarias, reglamentarias o contractuales relativas a la seguridad de la información o de los requisitos de seguridad.
- (b) Garantizar que la seguridad de la información se implementa y opera de acuerdo con la política y procedimientos de la Entidad.

5.13.2. Política

- (a) Todos los órganos y unidades orgánicas de IGP deben cumplir con todos los requisitos legislativos, regulaciones y requerimientos contractuales relativas a seguridad de la información, asimismo, deben ser identificadas y documentadas.
- (b) Todos los órganos y unidades orgánicas de IGP deben asegurar el cumplimiento a los derechos de propiedad intelectual, para lo cual todo el software que utiliza en la Entidad debe contar con la respectiva licencia de uso.
- (c) Los servidores del IGP no deben destruir o eliminar registros o información importante, sin la aprobación respectiva de los propietarios de información.
- (d) El IGP a través del Órgano o Unidad Orgánica responsable de acuerdo a su competencia, debe de garantizar la protección y la privacidad de los datos personales conforme a la legislación aplicable.
- (e) El IGP a través del Órgano o Unidad Orgánica responsable de acuerdo a su competencia, debe establecer los términos, condiciones y finalidades para datos personales en cumplimiento con la Ley existente y su Reglamento.
- (f) La Oficina de Tecnologías de la Información y Datos Geofísicos del IGP, debe asegurar que la seguridad de la información esté implementada y operada, a través de revisiones independientes de la seguridad de la información mediante auditorías para asegurar que se mantenga de forma eficaz, eficiente y efectiva.

	LINEAMIENTO	Versión: 04
	LINEAMIENTO DE SEGURIDAD DE LA INFORMACIÓN	Código: LI 001-2020-IGP Sigla de Área: OTIDG


5.14. Política de Escritorio y Pantalla Limpia de Información

5.14.1. Objetivos

- (a) prevenir el acceso no autorizado, pérdida y/o daño de la información que se encuentra en los puestos de trabajo, equipos de cómputo, medios extraíbles, dispositivos de impresión y digitalización de documentos, durante y fuera del horario laboral, aplicados por los funcionarios y servidores.

5.14.2. Política

- (a) Al levantarse de su puesto de trabajo o al finalizar el día laboral, los escritorios deben permanecer despejados y libres de documentos físicos y/o medios extraíbles (Dispositivos de almacenamiento de información) que contengan información pública clasificada o pública reservada,
- (b) Todos los activos que contenga información deben guardarse en un lugar seguro y bajo llave. Los documentos y/o medios extraíbles con información pública también deben guardarse para evitar la pérdida de dicha información.
- (c) Los puestos de trabajo deben permanecer limpios y ordenados.
- (d) Cuando se imprima o digitalice documentos con información pública clasificada o pública reservada, éstos deben retirarse inmediatamente de dichos dispositivos (Impresoras o escáner).
- (e) Los dispositivos de impresión y digitalización deben permanecer limpios de documentos.
- (f) Los gabinetes, cajones y archivadores que contienen documentos y/o medios extraíbles con información pública, pública clasificada o pública reservada deben quedar cerrados durante la hora de almuerzo y al finalizar el día laboral.
- (g) La pantalla del computador (escritorio) no debe contener ningún tipo de archivo, salvo los accesos directos a las aplicaciones necesarias para que los funcionarios o servidores ejerzan sus funciones o cumplan sus obligaciones contractuales, según el caso.
- (h) Los documentos electrónicos que producen los funcionarios o servidores en el ejercicio de sus funciones o en el cumplimiento de sus obligaciones contractuales, según el caso, deben guardarse en la carpeta de almacenamiento en red dispuesta por la entidad.
- (i) Al levantarse del puesto de trabajo, se debe bloquear la sesión de los equipos de cómputo para proteger el acceso a las aplicaciones y servicios de la entidad.
- (j) El Equipo de Operaciones de TI de la OTIDG, implementa el bloqueo automático de la sesión del usuario mediante el directorio activo pasado los 10 minutos de inactividad en el equipo de cómputo.
- (k) Todos los equipos de cómputo y dispositivos de impresión y digitalización deben apagarse cuando no estén en uso.
- (l) Tanto la Oficina de Tecnologías de la información y Datos Geofísicos del IGP tienen la responsabilidad del cumplimiento total de la política de escritorio y pantalla limpia de información.

	LINEAMIENTO	Versión: 04
	LINEAMIENTO DE SEGURIDAD DE LA INFORMACIÓN	Código: LI 001-2020-IGP Sigla de Área: OTIDG


Descripción de los términos, elementos o características específicas que se aplican en cualquier etapa de las actividades que ejecuta la organización.

VI. RESPONSABILIDADES

La Oficina de Tecnologías de la Información y Datos Geofísicos del IGP, se encargará de verificar el cumplimiento del presente Lineamiento

VII. ANEXOS


- Incluye documentación complementaria para la aplicación de los lineamientos.

	LINEAMIENTO	Versión: 04
	LINEAMIENTO DE SEGURIDAD DE LA INFORMACIÓN	Código: LI 001-2020-IGP Sigla de Área: OTIDG

Anexo I CHECKLIST DE CONFIGURACIÓN DE SEGURIDAD DE DISPOSITIVOS MÓVILES


Usuario y Equipo:

	Para todo dispositivo móvil:	Conforme	No Conforme
1	Autenticación de acceso configurada (contraseña mayor a 4 dígitos y/o biométrica)		
2	Último escaneo de antivirus o aplicación de seguridad del SO no indica acciones pendientes ante amenazas		
3	No tiene actualizaciones de seguridad pendientes		
	Para computadoras portátiles:		
4	Antivirus actualizado, licenciado y activado		
5	Libre de software prohibido por la institución		
	Para teléfonos móviles y tablets:		
6	Contar con la última versión disponible del SO		
7	Aplicación de seguridad del sistema operativo activada, por ejemplo, Google Play Protect		
8	No se tienen aplicaciones sospechosas, con permisos excesivos		
	Otros requisitos Ad Hoc		
Acciones tomadas ante requisitos no conformes			
Resultado final	Aprobado		No aprobado


	LINEAMIENTO	Versión: 04
	LINEAMIENTO DE SEGURIDAD DE LA INFORMACIÓN	Código: LI 001-2020-IGP Sigla de Área: OTIDG

Anexo II USO ACEPTABLE DE ACTIVOS DE INFORMACIÓN


Uso Aceptable
Utilizar los dispositivos institucionales para labores y actividades relacionadas directamente con las funciones del puesto y los objetivos institucionales.
Salvaguardar la información interna y la información confidencial (usuarios y contraseñas, URLs, datos personales, documentos internos, etc.)
Respetar las configuraciones establecidas por los administradores de los sistemas.
Cumplir con las políticas para contraseñas, trabajo remoto, de acceso y otras que emita la institución.
Cuidar la infraestructura física (instalaciones, hardware, elementos de las redes de comunicaciones) de modo que se evite su fallo prematuro.
Notificar a OTIDG ante cualquier dificultad a nivel lógico o físico y seguir las instrucciones que se proporcionan.
Uso Inaceptable - Prohibiciones
Realizar copias no autorizadas de información
Permitir que queden documentos físicos expuestos en el escritorio
Está prohibido proporcionar datos de usuario/contraseña o facilitar el acceso a los sistemas de la institución a terceros, ya sea deliberadamente o por error; esto incluye anotar las contraseñas en papel, en archivos digitales u otros soportes no autorizados
Revelar o publicar datos personales de servidores de la institución
Acceder o intentar acceder a datos, servidores, cuentas para las que no tiene permiso
Introducción de malware (virus, gusanos, adware, entre otros)
Instalar o intentar instalar software no autorizado.
Usar los equipos de cómputo para realizar tareas ajenas a las encargadas por la institución.
Realizar pruebas de seguridad a los sistemas de la institución sin estar autorizado
El ingreso y utilización de dispositivos de almacenamiento masivo, tales como memorias USB, discos duros portátiles, tarjetas de memoria y similares
El acceso o intento de acceso a sitios web de mala reputación, sospechosos o potencialmente peligrosos
Publicar en redes sociales opiniones personales que pueden parecer o confundirse con la posición de la institución


	LINEAMIENTO	Versión: 04
	LINEAMIENTO DE SEGURIDAD DE LA INFORMACIÓN	Código: LI 001-2020-IGP Sigla de Área: OTIDG

Envío de SMS, mensajes o correos electrónicos ajenos a las actividades institucionales
Acceder físicamente a zonas o ambientes para los que no se está autorizado.
Acceder a las instalaciones fuera del horario laboral sin tramitar los permisos correspondientes
No utilizar el fotocheck en las instalaciones.
Intentar resolver un problema propio de la competencia de los administradores de los sistemas, esto incluye tratar de acceder a configuraciones de nivel administrador o abrir y manipular elementos de hardware.

	LINEAMIENTO	Versión: 04
	LINEAMIENTO DE SEGURIDAD DE LA INFORMACIÓN	Código: LI 001-2020-IGP Sigla de Área: OTIDG

Anexo III ELIMINACIÓN DE MEDIOS REMOVIBLES

N°	Actividades
1	El personal que realiza la gestión patrimonial entrega el medio a la Oficina de Tecnologías de la Información y Datos Geofísicos del IGP
2	El personal de la Oficina de Tecnologías de la Información y Datos Geofísicos del IGP realiza una revisión; de concluir que el medio no está operativo
3	<p>De ser factible, sobre escribir manualmente el íntegro de la capacidad disponible del medio</p> <p>De ser posible lo anterior, realizar formateo de bajo nivel</p> <p>Para discos duros, de no ser viables las opciones anteriores por algún daño electrónico o físico del disco duro, aplicar la destrucción física por medio de realizar dos agujeros con un taladro directamente sobre los platos del disco (ver fotografía; usar lentes de seguridad para esta tarea).</p> 
4	Se comunica la baja al personal que realiza control patrimonial
5	El personal que realiza control patrimonial almacena el medio.
6	El personal que realiza control patrimonial realiza la disposición del medio.

	LINEAMIENTO	Versión: 04
	LINEAMIENTO DE SEGURIDAD DE LA INFORMACIÓN	Código: LI 001-2020-IGP Sigla de Área: OTIDG

Anexo IV ESTÁNDAR DE CONTRASEÑAS

Aplicar los siguientes requisitos cuando se crean o modifican contraseñas

1. Longitud mínima:


Grupo	Longitud mínima
Administradores de sistemas y servicios	10 caracteres
Otros usuarios	8 caracteres

2. Requisitos de complejidad:

- Restricciones:
 1. No utilizar contraseñas ya utilizadas en cuentas personales
 2. No utilizar una sola palabra, por ejemplo “Princesa85” o una frase conocida como “Iloveyou4ever”
 3. No deben contener el nombre de la cuenta del usuario
 4. No deben contener el/los nombre(s) o apellido(s) del usuario
 5. No se permitirá el uso de contraseñas que contengan las contraseñas más débiles: 12345678, 1qaz2wsx, qwertyuiop, password, contraseña y otras reconocidas.
- La contraseña debe contener caracteres de tres de las siguientes categorías:

Requisito	Administradores de sistemas y servicios	Otros usuarios
Al menos una letra mayúscula	X	X
Al menos una letra minúscula	X	X
Al menos un número del 0 al 9	X	X
Caracteres especiales	X	

3. El historial de contraseñas se establecerá en 12 para prevenir la reutilización de contraseñas.
4. La vigencia máxima de las contraseñas será de 180 días desde el último cambio de la contraseña.

	LINEAMIENTO	Versión: 04
	LINEAMIENTO DE SEGURIDAD DE LA INFORMACIÓN	Código: LI 001-2020-IGP Sigla de Área: OTIDG

Anexo V GUÍA PARA LA CLASIFICACIÓN Y MANEJO DE ACTIVOS DE INFORMACIÓN

1. OBJETIVO

La clasificación de activos de información tiene como objetivo asegurar que la información reciba los niveles de protección adecuados con base a la clasificación realizada por sus características particulares de cada activo en el inventario de activos de información, que permitan alcanzar los niveles apropiados de integridad, disponibilidad y confidencialidad en la seguridad de la información.

2. ALCANCE


El presente documento aplica para la clasificación de todos los activos de Información de la Institución y en general cualquier tipo de Información proveniente de terceras partes (cliente, proveedores, etc.) o generada internamente como resultados de los procesos internos de la institución en el marco del Sistema de Gestión de Seguridad de la Información.

3. DISPOSICIONES Y CONDICIONES GENERALES

La clasificación de la información que se define en la entidad se basa en las características particulares de la información, así mismo se busca dar cumplimiento a los requerimientos relacionados en la Gestión de Activos del Sistema de Gestión de Seguridad de la Información bajo el ISO 27001.

4. DEFINICIONES

- **Información:** Es un activo esencial para las actividades de la organización y en consecuencia necesita una protección adecuada. Es un activo esencial para las actividades de la organización y en consecuencia necesita una protección adecuada.
- **Activo de Información:** Recurso de información que tiene valor para la organización y sus clientes.
- **Clasificación de la Información:** La información debe clasificarse en términos de la sensibilidad y la importancia para la organización y sus clientes. Es el ejercicio por medio del cual se determina que la información pertenece a uno de los niveles de clasificación estipulados en la Entidad y tiene como objetivo asegurar que la información reciba el nivel de protección adecuado.
- **Información Confidencial:** Aquella información que es considerada como confidencial de acuerdo a lo establecido en el Texto Único Ordenado de la Ley 27806, Ley de transparencia y Acceso a la Información Pública.
- **Información Pública:** Aquella información que es de acceso público de acuerdo a lo establecido en el Texto Único Ordenado de la Ley N° 27806, Ley de Transparencia y Acceso a la Información Pública.

	LINEAMIENTO	Versión: 04
	LINEAMIENTO DE SEGURIDAD DE LA INFORMACIÓN	Código: LI 001-2020-IGP Sigla de Área: OTIDG

- **Propietario del activo de la Información:** Se designa como propietario de la Información para cada área de apoyo o unidad de negocio, a cada uno de los responsables quienes pueden tomar decisión sobre el activo de información.
- **Custodio de la Información:** Se establecen como custodios de la información a los empleados o terceros que conservan en su poder cualquier tipo de información proveniente de clientes, o generada internamente como resultado de los procesos internos de la organización. El custodio de la Información es el responsable de salvaguardar la información a su cargo de acuerdo a su clasificación para evitar pérdida o divulgación inadecuada mediante el cumplimiento de los controles establecidos.
- **Usuarios finales:** Los usuarios finales están definidos como todo empleado o tercero que tiene acceso autorizado a información o sistemas informáticos que sean propiedad o que sean administrados por la organización.
- **Confidencialidad:** Propiedad que determina que la información sólo esté disponible y sea revelada a individuos, entidades o procesos autorizados.
- **Integridad:** Propiedad de salvaguardar la exactitud y estado completo de los activos.
- **Disponibilidad:** Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada, cuando ésta así lo requiera.

5. INVENTARIO DE ACTIVOS


La realización del inventario de activos de información permite clasificar los activos a los que se les debe brindar mayor protección.

Las actividades a realizar para obtener un inventario de activos de información son la Definición, Revisión, Actualización y Publicación, los cuales se ven reflejados en la Matriz de Inventario de Activos de Información (PR N° 001-F01 Gestión de Activos de Información).

5.1. DEFINICIÓN

La definición consiste en determinar qué activos de información harán parte del inventario, esta tarea debe ser liderada por el Oficial de Seguridad y el líder de cada proceso, conjuntamente con un equipo que realice la gestión de activos de información.

Es recomendable que la definición del inventario se lleve a cabo por lo menos una vez al año.

	LINEAMIENTO	Versión: 04
	LINEAMIENTO DE SEGURIDAD DE LA INFORMACIÓN	Código: LI 001-2020-IGP Sigla de Área: OTIDG

5.2. REVISIÓN

En general, el inventario de activos puede ser revisado o validado en cualquier momento siempre en cuando lo solicite el líder o dueño del proceso (quien haga sus veces), o si el equipo de gestión de activos liderados por el Oficial de Seguridad de la Información así lo requiere.

Las razones por las cuales debería realizarse una revisión o validación son:

- Actualización del proceso al que pertenece el activo.
- Inclusión de un nuevo activo.
- Inclusión de nuevos registros, materiales o de referencia o procedimientos.


5.3. PUBLICACIÓN

El inventario de activos de información debe ser un documento clasificado como “Confidencial”, y no debe tener características que permitan modificarse por usuarios no autorizados. Sólo debe tener acceso de modificación a este documento el líder del proceso y/o a quien se delegue con previa autorización y conocimiento del oficial de seguridad de la información de la Entidad.

6. CLASIFICACIÓN DE LA INFORMACIÓN

Se considera Información Pública: aquella información que es de acceso público de acuerdo a lo establecido en el Texto Único Ordenado de la Ley N° 27806, Ley de Transparencia y Acceso a la Información Pública. El IGP cataloga esta información en Información Pública e Información de Uso Interno.


Se considera Información Confidencial: aquella información que es considerada como confidencial de acuerdo a lo establecido en el Texto Único Ordenado de la Ley 27806, Ley de Transparencia y Acceso a la Información Pública.

	LINEAMIENTO	Versión: 04
	LINEAMIENTO DE SEGURIDAD DE LA INFORMACIÓN	Código: LI 001-2020-IGP Sigla de Área: OTIDG

ESQUEMA DE CLASIFICACIÓN

	INFORMACIÓN PÚBLICA		INFORMACIÓN CONFIDENCIAL
	PÚBLICA	INTERNO	
DEFINICIÓN	Aquella que de acuerdo a la normativa nacional vigente se encuentra publicada en el Portal de Transparencia estándar.	Esta información se maneja según las competencias de las unidades orgánicas, estableciendo permisos de lectura / escritura para evitar modificaciones no intencionales.	Aquello que incluye datos de carácter personal y sensible de servidores, clientes y demás personas naturales sobre las cuales el IGP efectúa algún tratamiento de información para un fin determinado declarado como banco de datos personales entre otros. Aquello que incluye datos de carácter sensible y uso exclusivo sobre comunicación, procesos, servicios, sistemas, entre otros.
EJEMPLO	Publicaciones, anuncios de oportunidades de trabajo, comunicados de prensa, folletos de productos.	Aquella información que se encuentra en la Intranet de la Entidad, presupuestos departamentales, manuales o políticas internas.	Usuarios y contraseñas a los sistemas; valores de contratación, información personal, reportes de vulnerabilidades, documentación del funcionamiento y la configuración de los sistemas.
CONTROL	<ul style="list-style-type: none"> Ninguna restricción para el acceso de lectura. se debe manejar de modo que tenga altos niveles de disponibilidad. El acceso de actualización y eliminación debe ser autorizado por el propietario de la información. 	<ul style="list-style-type: none"> Debe estar protegido de acuerdo al cuadro de controles aplicables de acuerdo al numeral 9 de este documento. 	

7. PROCEDIMIENTO PARA EL ETIQUETADO DE ACTIVOS DE INFORMACIÓN

	LINEAMIENTO	Versión: 04
	LINEAMIENTO DE SEGURIDAD DE LA INFORMACIÓN	Código: LI 001-2020-IGP Sigla de Área: OTIDG

- Los propietarios de activos de información son responsables de clasificar la información que manejan en cada proceso o proyecto de acuerdo a lo establecido en la Ley de Transparencia y Acceso a la Información Pública.
- Los propietarios de los activos de información deberán etiquetar la información según la clasificación realizada.
- La información confidencial será etiquetada inicialmente en el documento que se utilice para realizar el inventario de activos de información.
- Se aplicarán etiquetas en los metadatos asociados a la información en caso se trate de información almacenada en medios digitales.
- Se etiquetarán todos los activos de información que estén clasificados según el esquema de clasificación como Confidenciales.
- Se etiquetará el nivel de clasificación en relación a Confidencialidad y deberá figurar textualmente la palabra CONFIDENCIAL.
- La información pública (pública e interna) no necesita etiqueta.
- Si un activo de información en formato impreso no se encuentra etiquetado debe ser tratado en todos sus niveles (Confidencialidad, Integridad y Disponibilidad) como No clasificado.

8. MANEJO DE LOS ACTIVOS DE INFORMACIÓN

Los servidores deben usar los activos de información para los fines y objetivos del IGP de acuerdo con los documentos normativos y procedimientos definidos en el Uso aceptable de activos de información.

En el caso almacenamiento y/o de traslado de los activos de información, se debe cumplir con los documentos normativos específicos de la entidad:

- Directiva N° 05-OGA-IGP/2014 Norma y Procedimiento para el uso, cuidado y salida de bienes del IGP.
- Directiva N° 006-2018-IGP/SG-OAD Control de ingresos y salidas en los locales del IGP.
- La custodia y el acceso al mismo, de los activos de información Confidencial de forma físico, solo debe ser por personal autorizado.
- Los ambientes donde se almacenen información confidencial de forma física, debe ser tratado como un área restringida.

9. CONTROLES APLICABLES PARA LOS ACTIVOS DE INFORMACIÓN SEGÚN LA CLASIFICACIÓN DE LA INFORMACIÓN