

	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	PSIG-031
		Edición: 04
		Fecha: 10/09/26
		Página 1

Contenido

1. CONTEXTO DE LA ORGANIZACIÓN	3
1.1. ORGANIZACIÓN Y SU CONTEXTO	3
1.2. NECESIDADES Y EXPECTATIVAS DE LAS PARTES INTERESADAS	3
2. MISIÓN, VISIÓN Y VALORES	5
2.1. MISIÓN	5
2.2. VISIÓN	5
2.3. VALORES	5
3. SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	6
3.1. PRINCIPIOS DE SEGURIDAD DE LA INFORMACIÓN	6
3.2. DECLARACIÓN DE APLICABILIDAD	6
3.3. DETERMINACIÓN DEL ALCANCE DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	7
3.4. POLÍTICAS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	7
3.5. OBJETIVO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	8
3.6. ROLES Y RESPONSABILIDADES	8
3.7. COMITÉ DE SEGURIDAD DE LA INFORMACIÓN	10
4. INFORMACIÓN DE SEGURIDAD DE LOS CONTROLES	11
5. GESTIÓN DE RIESGOS	11
6. CAPACITACIÓN Y CONCIENCIACIÓN	12
7. REVISIÓN Y MEJORA CONTINUA	12
8. DESCRIPCIÓN DE LAS POLÍTICAS	13
8.1. POLÍTICA DE GESTIÓN DE LA INFORMACIÓN Y CICLO DE VIDA	13
8.2. POLÍTICA DE CONTROL DE ACCESO Y TRAZABILIDAD	13
8.3. POLÍTICA DE GESTIÓN E INVENTARIO DE ACTIVOS	14
8.4. POLÍTICA PARA LA GESTIÓN DEL TALENTO Y CULTURA DE SEGURIDAD	14
8.5. POLÍTICA DE MANEJO DEL RIESGO	14
8.6. POLÍTICA DE SEGURIDAD FÍSICA, PERIMETRAL Y AMBIENTAL	15
8.7. POLÍTICA DE GESTIÓN DE LAS REDES Y LOS SISTEMAS INFORMÁTICO	15
8.8. POLÍTICA DE RESPALDO, CONTINUIDAD Y RECUPERACIÓN	16

<i>Elaboró:</i> Isadora Morales Villegas Responsable SIG	<i>Revisó:</i> Marcel Capafons Responsable del Sistema	<i>Aprobó:</i> Alex Martínez Gerencia General
--	--	---

	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	PSIG-031
		Edición: 04
		Fecha: 10/09/26
		Página 2

8.9.	POLÍTICA DE GESTIÓN DE LOS INCIDENTES y CSIRT	16
8.10.	POLÍTICA RELACIÓN CON TERCEROS Y CUMPLIMIENTO LEGAL	16
9.	SANCIÓN Y CUMPLIMIENTO	17
10.	AUDITORÍA	17
12.	ANEXOS	17
13.	CONTROL DE CAMBIOS	17

<i>Elaboró:</i> Isadora Morales Villegas Responsable SIG	<i>Revisó:</i> Marcel Capafons Responsable del Sistema	<i>Aprobó:</i> Alex Martínez Gerencia General
--	--	---

	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	PSIG-031
		Edición: 04
		Fecha: 10/09/26
		Página 3

1. CONTEXTO DE LA ORGANIZACIÓN

1.1. ORGANIZACIÓN Y SU CONTEXTO

INTEL es una empresa de servicios que suministra a sus clientes, desde hace más de 50 años, una solución integrada y completa a sus comunicaciones de empresa, dotándoles de las últimas tecnologías en el mercado de las telecomunicaciones. Un mercado cuya dinámica exige una evolución y formación constante. Consciente del compromiso con sus clientes y la importancia de la seguridad integral, ha establecido un Sistema de Gestión de Seguridad de la Información.

El personal de INTEL dispone de la máxima calificación y experiencia para desarrollar sus funciones, así como las herramientas y tecnología necesarias para asegurar la calidad y eficiencia en sus actuaciones.

Dado que el entorno es cambiante, INTEL asume el compromiso de analizar el contexto interno y externo de la organización de forma periódica, incluyendo cuestiones relacionadas como el cambio climático, normativa legal, o cualquier otro tema que pueda impactar en la sostenibilidad y resiliencia en la organización.

1.2. NECESIDADES Y EXPECTATIVAS DE LAS PARTES INTERESADAS

INTEL ha analizado y determinado las partes interesadas y los requisitos pertinentes de las mismas para el Sistema de Gestión de Seguridad de la Información, resultando:

- Clientes: Expectativas en la calidad de nuestros productos y servicios, seguridad y confiabilidad de la información, protección de sus datos personales y cumplimiento de los acuerdos de nivel de servicio, al igual que la capacidad de respuesta a incidencias en el servicio y de seguridad, eventualidades por el cambio climático. Productos y servicios que cumplan con todas las exigencias legales. Debemos cuidar la fidelización y seguimiento del grado de satisfacción.

<i>Elaboró:</i> Isadora Morales Villegas Responsable SIG	<i>Revisó:</i> Marcel Capafons Responsable del Sistema	<i>Aprobó:</i> Alex Martínez Gerencia General
--	--	---

	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	PSIG-031
		Edición: 04
		Fecha: 10/09/26
		Página 4

- Fabricantes/ partners: Los temas más relevantes a tener en cuenta son las alianzas estratégicas y el cumplimiento de los requisitos de calidad, seguridad y confiabilidad establecidas. Expectativa por el cumplimiento de las condiciones de cada partner en la relación comercial, como, por ejemplo, el nivel de desempeño objetivo y certificaciones. Cumplimiento de los requisitos legales pertinentes y de seguridad de la información.
- Propiedad de la empresa: Expectativas en la sostenibilidad, continuidad del negocio, generando rentabilidad a los accionistas, en el marco del cumplimiento legal y normativo. Generación de nuevos modelos de negocio en seguridad de la información, ciberseguridad y protección de la privacidad. Empresa legalmente al día.
- Personal: Cumplimiento de normativas y requisitos de seguridad y salud laboral, oportunidades de desarrollo profesional, formación en seguridad de la información, ciberseguridad y protección de la privacidad, entorno de trabajo seguro, adecuación de competencias, y satisfacción del personal con el ambiente de trabajo.
- Competencia: INTEL considera muy importante hacer una investigación de la competencia para evitar ser desbancados y estar alerta en cuanto a innovación y desarrollo, imagen de la marca, certificaciones obtenidas y posicionamiento en el mercado.
- Sociedad: Debemos considerar, el impacto de nuestra actividad en la sociedad, en la demanda de servicios seguros contra ciberataques, la protección de los datos personales, la continuidad de los servicios esenciales, además de velar por nuestra imagen corporativa.
- Administraciones públicas / Autoridades: Debemos cumplir con todos los requisitos legales y reglamentarios de aplicación, como la protección de datos, la ciberseguridad, además, de los requisitos de notificación de incidentes, sostenibilidad, y continuidad del negocio.

Elaboró: Isadora Morales Villegas Responsable SIG	Revisó: Marcel Capafons Responsable del Sistema	Aprobó: Alex Martínez Gerencia General
--	--	---

	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	PSIG-031
		Edición: 04
		Fecha: 10/09/26
		Página 5

2. MISIÓN, VISIÓN Y VALORES

2.1. MISIÓN

Aportar valor a las empresas. Ponemos a disposición de nuestros clientes las mejores soluciones TIC empresariales que faciliten el desarrollo y mejoren la productividad de sus negocios, en el marco de la seguridad integral.

2.2. VISIÓN

Queremos ser un referente nacional en el ámbito de soluciones TIC para empresas con seguridad integral, destacando por la calidad y eficiencia de nuestros servicios profesionales. Aportando rentabilidad a los accionistas y creando un proyecto motivador y apetecible a nuestros empleados.

“Nos comprometemos a proteger la confidencialidad, integridad y disponibilidad de la información en todas nuestras actividades.”

2.3. VALORES

- ✓ **Orientación al cliente:** Ponemos tu experiencia en el centro de nuestra estrategia. Comprometidos con la calidad, guiados por la seguridad
- ✓ **Implicación:** Mediante un servicio de calidad, contribuyendo en la seguridad de la información y generación de valor.
- ✓ **Trabajo en equipo:** Con la fortaleza del trabajo en equipo
- ✓ **Honestidad:** Con soluciones que se adaptan a tus necesidades reales.
- ✓ **Profesionalidad:** Focalizado en la excelencia y el know-how tecnológico.
- ✓ **Capacidad de autocrítica:** Y la mejora continua en nuestros procesos
- ✓ **Compromiso con nuestra sociedad:** Actuando de manera responsable y transversal para ser un agente de cambio

<i>Elaboró:</i> Isadora Morales Villegas Responsable SIG	<i>Revisó:</i> Marcel Capafons Responsable del Sistema	<i>Aprobó:</i> Alex Martínez Gerencia General
--	--	---

	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	PSIG-031
		Edición: 04
		Fecha: 10/09/26
		Página 6

3. SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

La Dirección de Infraestructuras y Sistemas de Telecomunicación, S.L. en adelante, INSTEL, consciente del compromiso con sus clientes y la importancia de la seguridad integral, establece, implementa, mantiene y mejora de manera continua el sistema de seguridad de la información, ciberseguridad y protección de la privacidad, en adelante, Sistema de Gestión de Seguridad de la Información, SGSI, de acuerdo con los requisitos establecidos, tomando las medidas adecuadas para la protección frente a daños accidentales o deliberados que puedan afectar la disponibilidad, integridad, confidencialidad, trazabilidad y autenticidad de la información.

3.1. PRINCIPIOS DE SEGURIDAD DE LA INFORMACIÓN

- **Autenticidad:** Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.
- **Confidencialidad:** Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados.
- **Disponibilidad:** Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren.
- **Integridad:** Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada.
- **Trazabilidad:** propiedad o característica consistente en que las actuaciones de una entidad (persona o proceso) pueden ser trazadas de forma indiscutible hasta dicha entidad.

3.2. DECLARACIÓN DE APLICABILIDAD

Ver: PSIG-031.A01 DECLARACIÓN DE APLICABILIDAD SGSI_V3

<i>Elaboró:</i> Isadora Morales Villegas Responsable SIG	<i>Revisó:</i> Marcel Capafons Responsable del Sistema	<i>Aprobó:</i> Alex Martínez Gerencia General
--	--	---

	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	PSIG-031
		Edición: 04
		Fecha: 10/09/26
		Página 7

3.3. DETERMINACIÓN DEL ALCANCE DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

El alcance definido por INTEL es:

“Sistema de Gestión de Seguridad de la Información, ciberseguridad y protección de la privacidad que da soporte a la prestación de los servicios que abarca la consultoría, instalación, integración, y mantenimiento de los sistemas informáticos, de telecomunicaciones e infraestructuras IT y externalización de tareas IT, conforme a la declaración de aplicabilidad de fecha 10 de septiembre del 2026.”

3.4. POLÍTICAS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

La Política del Sistema de Gestión de Seguridad de la Información de XX, establecida por la Gerencia General y de obligatorio cumplimiento para toda la organización, refleja el compromiso ético y responsable de proteger la información procesada y/o almacenada dentro del alcance definido del SGSI. Asimismo, garantiza la adecuada gestión de la seguridad de la información y el cumplimiento de los requisitos legales, regulatorios, contractuales y organizacionales aplicables, promoviendo la confidencialidad, integridad y disponibilidad de la información.

Para desarrollar esta política, la dirección de INTEL se compromete a:

- Llevar a cabo un **análisis de riesgos** periódico que permita mantener una adecuada visión de los riesgos de seguridad de la información a los que están expuestos los activos y desarrollar las medidas necesarias para limitar y reducir dichos riesgos, definiendo las medidas de seguridad a establecer.
- Desarrollar una completa **normativa de seguridad** que regule las condiciones en las que la empresa, dentro del alcance establecido, debe desarrollar su actividad para respetar los requerimientos de seguridad establecidos.
- Destinar los **recursos y medios necesarios** para desarrollar todas las medidas de seguridad que se determinen, manteniendo un adecuado balance entre coste y beneficio.

Elaboró: Isadora Morales Villegas Responsable SIG	Revisó: Marcel Capafons Responsable del Sistema	Aprobó: Alex Martínez Gerencia General
--	--	---

	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	PSIG-031
		Edición: 04
		Fecha: 10/09/26
		Página 8

- Establecer un **plan de formación y concienciación** en materia de seguridad de la información que ayude a todo el personal implicado a conocer y cumplir las medidas de seguridad establecidas y a participar de forma proactiva en la gestión de la seguridad de la información.
- Desarrollar todas las medidas necesarias para garantizar la adecuada **gestión de los incidentes** de seguridad que puedan producirse, y que permitan la resolución tanto de las incidencias menores como de las situaciones que puedan poner en riesgo la continuidad de las actividades contempladas.
- Establecer periódicamente un conjunto de **objetivos e indicadores** en materia de seguridad de la información que permitan el adecuado seguimiento de la evolución de la seguridad dentro de la empresa.
- Establecer una **metodología de revisión, auditoría y mejora continua** del sistema, siguiendo un ciclo PHVA que garantice el mantenimiento continuo de los niveles de seguridad deseados. INSTEL establece los procedimientos y formas de actuación necesarias para garantizar el correcto desarrollo de esta política, que se plasman en un sistema de seguridad, documentado y conocido por todo el personal de INSTEL, y que cumple los requisitos establecidos en la norma.

3.5. OBJETIVO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.

- 3.5.1.** Garantizar la disponibilidad de los activos de información corporativos y continuidad operativa.
- 3.5.2.** Fortalecer la resiliencia operativa y la capacidad de respuesta ante incidentes de seguridad de la información.
- 3.5.3.** Fomentar una cultura organizativa orientada a la seguridad de la información y la gestión responsable de los activos.

3.6. ROLES Y RESPONSABILIDADES

Con el fin de asegurar una gestión eficaz de los componentes del Sistema de Gestión de Seguridad de la Información (SGSI), se establece una estructura organizacional que define los roles requeridos y sus respectivas responsabilidades.

<i>Elaboró:</i> Isadora Morales Villegas Responsable SIG	<i>Revisó:</i> Marcel Capafons Responsable del Sistema	<i>Aprobó:</i> Alex Martínez Gerencia General
--	--	---

	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	PSIG-031
		Edición: 04
		Fecha: 10/09/26
		Página 9

Los roles descritos no necesariamente corresponden a los cargos definidos en el organigrama de XX; por lo tanto, una misma persona podrá asumir las responsabilidades asociadas a uno o más roles, siempre que se garantice la adecuada segregación de funciones y el cumplimiento de los controles establecidos.

La Gerencia General es responsable de definir y aprobar los roles de seguridad de la información, así como sus funciones, responsabilidades y autoridades. Asimismo, determinará los mecanismos para su designación, renovación y actualización, dejando evidencia de ello mediante las actas del Comité de Seguridad de la Información o los registros correspondientes, donde se formalicen los nombramientos, cambios, incorporaciones o retiros de sus integrantes.

3.6.1. Organigrama del SGSI

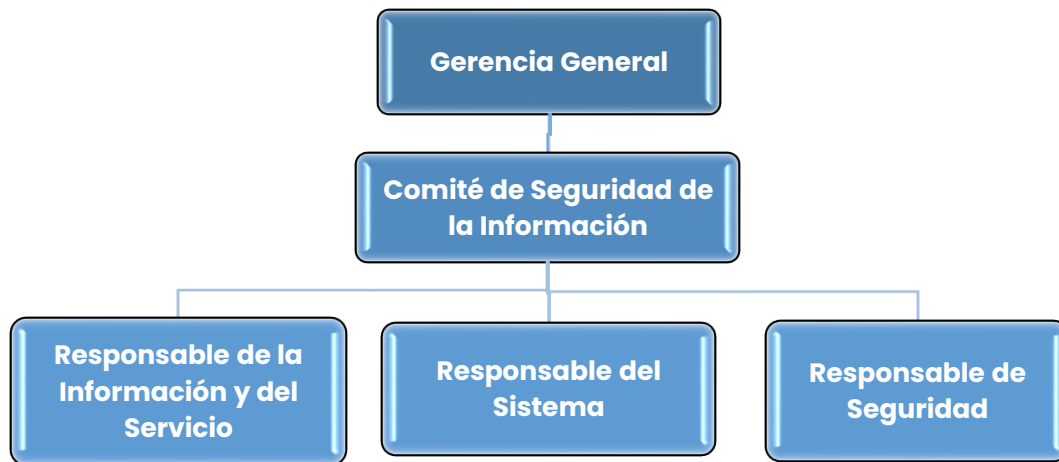
De acuerdo con la estructura organizacional de Instel, todos los cargos reportan a la Dirección Financiera y de Operaciones, la cual ejerce la supervisión y coordinación de las actividades empresariales.

El área de Tecnología de la Información (TI) está conformada por el Responsable de la Información y el Servicio, así como por el Responsable de Sistemas, quienes tienen a su cargo la gestión, administración y protección de los recursos tecnológicos y de información de la organización.

Para garantizar la adecuada operación, seguimiento y mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI), a continuación, se presenta el organigrama funcional que define las líneas de responsabilidad y autoridad asociadas a la seguridad de la información.

<i>Elaboró:</i> Isadora Morales Villegas Responsable SIG	<i>Revisó:</i> Marcel Capafons Responsable del Sistema	<i>Aprobó:</i> Alex Martínez Gerencia General
--	--	---

	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	PSIG-031
		Edición: 04
		Fecha: 10/09/26
		Página 10



3.7. COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

El Comité de Seguridad de la Información tiene como objetivo la supervisión, alineación y mejora continua del SGSI en el marco de la norma ISO/IEC 27001.

3.7.1. Funciones

- Establecer las políticas y lineamientos para planear, organizar, dirigir, controlar y coordinar las actividades relacionadas con la Política de Seguridad, con el fin de garantizar la aplicación de los principios y directrices establecidas en las normas que regulan la materia.
- Revisar los lineamientos técnicos y operativos para la implementación del Sistema de Gestión de Seguridad de la Información (SGSI), con base en el Manual y la Política.
- Aprobar los roles y responsabilidades del SGSI: responsable de la información y del servicio, responsable de la seguridad y el responsable del sistema.
- Soportar la administración y desarrollo de iniciativas de seguridad de la información a través de compromisos y de la disponibilidad de recursos, así como la formulación, actualización y divulgación de la política de seguridad de la información al interior de la entidad.
- Generar recomendaciones para la formulación, adecuación y aprobación de políticas, planes, programas y proyectos en materia de seguridad de la información y controles específicos de seguridad para la implementación de nuevos servicios

<i>Elaboró:</i> Isadora Morales Villegas Responsable SIG	<i>Revisó:</i> Marcel Capafons Responsable del Sistema	<i>Aprobó:</i> Alex Martínez Gerencia General
--	--	---

	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	PSIG-031
		Edición: 04
		Fecha: 10/09/26
		Página 11

- Revisar, analizar y recomendar las acciones que considere adecuadas frente a los incidentes de seguridad de la información en busca de la mejora continua.
- Con base en los resultados del análisis de riesgos de los activos de información, revisar y aprobar el plan de mitigación del riesgo que contribuya al mejoramiento continuo del SGSI.
- Realizar revisiones al SGSI periódicamente y, según los resultados de esta revisión, definir las acciones a seguir
- Velar por el cumplimiento de las políticas, normas, procedimientos y demás documentos relacionados con la seguridad de la información

3.7.2. Sesiones

El Comité de Seguridad de la Información se reunirá de forma ordinaria cada semestre, el segundo jueves de cada mes, de 9 a 10 de la mañana en la sala de reuniones de Instel, si o de forma extraordinaria cuando la Dirección General o los integrantes del comité lo soliciten, acorde con las circunstancias que así lo ameriten.

4. INFORMACIÓN DE SEGURIDAD DE LOS CONTROLES

- **Control de Accesos:** Definir y gestionar los niveles de acceso a la información y sistemas.
- **Seguridad en Redes:** Implementar medidas para proteger las redes de telecomunicaciones contra accesos no autorizados y ataques.
- **Gestión de Incidentes:** Establecer procedimientos para la detección, reporte y respuesta a incidentes de seguridad de la información a las autoridades competentes si procede.

5. GESTIÓN DE RIESGOS

La gestión del riesgo en un Sistema de Gestión de la Seguridad de la Información (SGSI) es un proceso integral y continuo que articula dos actividades fundamentales: el análisis de riesgos (para determinar los activos de la organización, evaluar su valor y estimar las consecuencias y probabilidad de las amenazas) y el tratamiento de los riesgos (para

<i>Elaboró:</i> Isadora Morales Villegas Responsable SIG	<i>Revisó:</i> Marcel Capafons Responsable del Sistema	<i>Aprobó:</i> Alex Martínez Gerencia General
--	--	---

	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	PSIG-031
		Edición: 04
		Fecha: 10/09/26
		Página 12

seleccionar e implantar salvaguardas que prevengan, mitiguen, compartan o acepten dichos riesgos).

Enmarcada dentro de la fase de planificación del ciclo de mejora continua (PDCA) del SGSI, su función ejecutiva es racionalizar la gestión de la seguridad, proporcionando a la Dirección un modelo fundamentado para tomar decisiones estratégicas alineadas con la misión de la organización y mantener el riesgo residual bajo límites formales y aceptables.

6. CAPACITACIÓN Y CONCIENCIACIÓN

Proveer programas de capacitación y concienciación en seguridad de la información, Ciberseguridad y Protección de la Privacidad, para todos los empleados y partes interesadas. Todo el personal recibirá formación periódica en:

- Principios básicos de seguridad de la información (confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad).
- Cumplimiento normativo y legal.
- Políticas y procedimientos internos.
- Gestión segura de contraseñas.
- Identificación y reporte de incidentes.
- Buenas prácticas en el uso de dispositivos y redes.
- Detección de amenazas y comportamientos sospechosos.

7. REVISIÓN Y MEJORA CONTINUA

La presente Política de Seguridad de la Información se concibe dentro de un marco dinámico de mejora continua (ciclo PDCA), reconociendo que los sistemas de información están sometidos a una evolución constante motivada por la aparición de nuevos activos, tecnologías y amenazas. La organización se compromete a mantener la seguridad de forma permanente y a reevaluar periódicamente la eficacia de sus medidas y análisis de riesgos, aprendiendo continuamente de la experiencia operativa y de los incidentes ocurridos. Asimismo, la política, la normativa y el modelo de gestión del riesgo se revisarán formalmente ante cualquier cambio sustancial en el contexto, en la arquitectura del sistema o en los requisitos legales y de negocio, asegurando que el riesgo residual permanezca siempre bajo los límites aceptables aprobados por la Dirección

<i>Elaboró:</i> Isadora Morales Villegas Responsable SIG	<i>Revisó:</i> Marcel Capafons Responsable del Sistema	<i>Aprobó:</i> Alex Martínez Gerencia General
--	--	---

	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	PSIG-031
		Edición: 04
		Fecha: 10/09/26
		Página 13

8. DESCRIPCIÓN DE LAS POLÍTICAS

Las políticas son una descripción del “que”, el cual se despliega a través de los lineamientos, guías y procedimientos. A continuación, se entregan las diferentes políticas de seguridad:

8.1. POLÍTICA DE GESTIÓN DE LA INFORMACIÓN Y CICLO DE VIDA

Esta política define los lineamientos para la transferencia, eliminación, destrucción y tratamiento seguro y controlado de información dentro y fuera de la organización, se aplica a todos los medios (digitales, físicos y verbales) y a todos los niveles de información, siendo su objetivo proteger la confidencialidad, integridad y disponibilidad según ISO/IEC 27001.

8.2. POLÍTICA DE CONTROL DE ACCESO Y TRAZABILIDAD

Todos y cada uno de los sistemas informáticos y plataformas tecnológicas debe contar con un adecuado control de acceso, en la medida que:

- Se tengan procedimientos para autorizar y revocar privilegios.
- Se tenga separación de funciones en el acceso
- Se tengan auditorías y registros de seguimientos en los sistemas de información y comunicaciones.
- Se cuente con control para el acceso remoto y redes inalámbricas.
- Se cuente con controles de acceso hacia los sistemas de información, que surtan la identificación y autorización respectiva.
- Se protejan las contraseñas y sistemas de autenticación.
- Se haga gestión sobre todos los privilegios de usuarios y la respectiva actualización de procedimientos.
- Todos los usuarios deben tener una identificación única, se prohíbe el préstamo de cualquier elemento de identificación y autenticación.

<i>Elaboró:</i> Isadora Morales Villegas Responsable SIG	<i>Revisó:</i> Marcel Capafons Responsable del Sistema	<i>Aprobó:</i> Alex Martínez Gerencia General
--	--	---

	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	PSIG-031
		Edición: 04
		Fecha: 10/09/26
		Página 14

8.3. POLÍTICA DE GESTIÓN E INVENTARIO DE ACTIVOS

Todos los activos de información que hagan parte del alcance de implementación, deben ser identificados, etiquetados e inventariados, para ello:

- Se debe definir la propiedad de los activos.
- Se debe contar con mecanismos para la clasificación.
- Artículo 21. Integridad y actualización del sistema.
- La inclusión de cualquier elemento físico o lógico en el catálogo actualizado de activos del sistema, o su modificación, requerirá autorización formal previa.

8.4. POLÍTICA PARA LA GESTIÓN DEL TALENTO Y CULTURA DE SEGURIDAD

La organización debe tener procedimientos para el reclutamiento, selección y desvinculación del personal, para lo cual:

- Se deben definir y mantener los roles y responsabilidades.
- Definir claramente las condiciones contractuales y de seguridad, incluyendo los acuerdos de confidencialidad.
- Entregar la debida identificación para el ingreso a los sistemas de información y revocar éstos cuando ya no se usen o la persona esté por fuera de la empresa.
- Se tengan procesos o un control disciplinario y/o administrativo que evalúen las faltas y den sanciones de acuerdo al estatuto de los trabajadores y el convenio colectivo vigente.
- Se deben tener planes de capacitación anual para los empleados y oficiales de seguridad, de modo que se eleven los niveles de sensibilización frente a la protección de la información.

8.5. POLÍTICA DE MANEJO DEL RIESGO

Se debe contar con una metodología de riesgos, para la identificación, análisis y evaluación, así como los mecanismos de tratamiento, para lo cual es necesario:

- Formalizar la metodología general de riesgos para el sistema de información.
- Definir los niveles aceptables de los riesgos por parte de la alta dirección.

<i>Elaboró:</i> Isadora Morales Villegas Responsable SIG	<i>Revisó:</i> Marcel Capafons Responsable del Sistema	<i>Aprobó:</i> Alex Martínez Gerencia General
--	--	---

	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	PSIG-031
		Edición: 04
		Fecha: 10/09/26
		Página 15

- Definir los roles y responsabilidades frente al riesgos.
- General mapas de riesgos al menos cada año, o cuando se identifiquen cambios relevantes en el SGSI

8.6. POLÍTICA DE SEGURIDAD FÍSICA, PERIMETRAL Y AMBIENTAL

Se deben tener elementos de protección física que resguardes los centros de datos y las redes en general:

- Se debe tener control de acceso físico a las instalaciones, que proteja contra amenazas internas y externas.
- Identificación del personal propio, proveedores y contratistas.
- Se debe medir las variables ambientales de los centros de cómputo como humedad y temperatura.
- Seguridad para los equipos informáticos que estén por fuera de las instalaciones.

8.7. POLÍTICA DE GESTIÓN DE LAS REDES Y LOS SISTEMAS INFORMÁTICO

Todas las redes de telecomunicaciones, sistemas informáticos, dispositivos móviles y sistemas de información deben contar con la protección adecuada ante ataques, fuga de información y accesos no autorizados:

- Se debe contar con sistemas EDR en todos los sistemas.
- Se debe tener un sistema de monitoreo de alertas de seguridad en toda la red y sistemas.
- Todos los servicios y acceso a la red deben estar controlados, para lo cual se debe implementar control de acceso en la red y sistemas de información.
- Los sistemas de red deben tener las configuraciones de seguridad (hardening) antes de estar en producción y tener servicio.
- Es obligatorio el bastionado de sistemas mediante salvaguardas de tipo [EL], diseñadas para anular vectores de ataque conocidos.

<i>Elaboró:</i> Isadora Morales Villegas Responsable SIG	<i>Revisó:</i> Marcel Capafons Responsable del Sistema	<i>Aprobó:</i> Alex Martínez Gerencia General
--	--	---

	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	PSIG-031
		Edición: 04
		Fecha: 10/09/26
		Página 16

8.8. POLÍTICA DE RESPALDO, CONTINUIDAD Y RECUPERACIÓN

La estrategia de continuidad debe basarse en un análisis de impacto de negocio BIA, que defina tiempos de recuperación realistas. Se deben tener sistemas de respaldo y procedimientos de recuperación, protección de medios de almacenamiento y control de acceso hacia las librerías y cintas.

- Todos los medios removibles o de almacenamiento que no se usen se les debe eliminar su información de modo seguro (sin recuperación).
- Tanto las bases de datos, aplicaciones como medios de almacenamiento deben ser respaldados de forma periódica.
- Se debe programar al menos una vez al año pruebas de restauración de copias de seguridad para garantizar la resiliencia operativa.

8.9. POLÍTICA DE GESTIÓN DE LOS INCIDENTES y CSIRT

Se debe contar con un proceso para la atención, detección, control, tratamiento y respuesta de incidentes de seguridad:

- Cada incidente debe alimentar las fuentes de los riesgos, con sus respectivos tratamientos.
- Se debe tener un equipo de respuesta a incidentes y/o un CSIRT.
- Todos los eventos de seguridad deben ser registrados y monitoreados hasta la solución final.
- Se debe contar con un procedimiento para la investigación.
- Se adopta una política de tolerancia cero y no negociación ante extorsiones y ransomware.

8.10. POLÍTICA RELACIÓN CON TERCEROS Y CUMPLIMIENTO LEGAL

Debe asegurarse en la gestión de proveedores, que las diferencia de las responsabilidades mediatas e inmediatas en la cadena de suministro, asegurando un marco de cumplimiento integrado, incluyendo mecanismos de supervisión y control continuos.

<i>Elaboró:</i> Isadora Morales Villegas Responsable SIG	<i>Revisó:</i> Marcel Capafons Responsable del Sistema	<i>Aprobó:</i> Alex Martínez Gerencia General
--	--	---

	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	PSIG-031
		Edición: 04
		Fecha: 10/09/26
		Página 17

9. SANCIÓN Y CUMPLIMIENTO

Cualquier incumplimiento de la política de seguridad y el modelo que la despliega, podrá conllevar medidas disciplinarias, sin perjuicio de las responsabilidades legales que pudieran derivarse.

10. AUDITORÍA

Realizar auditorías periódicas para asegurar el cumplimiento de la política y la efectividad del SGSI, y tomar acciones correctivas cuando sea necesario.

11. Liderazgo y Cultura

Promover la seguridad como una responsabilidad compartida, donde la Dirección lidere mediante el ejemplo y la asignación de recursos adecuados.

12. ANEXOS

- PSIG-031.A01 DECLARACIÓN DE APLICABILIDAD

13. CONTROL DE CAMBIOS

Edición	Fecha	Comentarios
01	16/06/2025	<i>Creación del documento para el SGSI</i>
02	7/08/2025	<i>Cambios en la política y objetivos del SGSI</i>
03	13/11/2025	<i>Nuevos objetivos SGSI 2025- 2026</i>
04	10/29/2026	<i>Actualización de la Declaración de Aplicabilidad.</i>

46349590J
ALEJANDRO
MARTINEZ (R:
B59524272)

Firmado digitalmente por 46349590J ALEJANDRO MARTINEZ (R: B59524272)
Nombre de reconocimiento (DN): 2.5.4.13=Reg-08005 / HojaB-8191 / Tomo-36672 / Folio-103 / Fecha-30/09/2015 / InscripciónB, serialNumber=IDCE-46349590J
givenName=ALEJANDRO, sn=MARTINEZ NICART, c=MX, o=INFRAESTRUCTURAS Y SISTEMAS DE TELECOMUNICACION SL, c=ES
Fecha: 2026.09.21 17:08:16 +02'00'

Elaboró: Isadora Morales Villegas Responsable SIG	Revisó: Marcel Capafons Responsable del Sistema	Aprobó: Alex Martínez Gerencia General
--	--	---