Contenido

1. CONTEXTO DE LA ORGANIZACIÓN

1.1. ORGANIZACIÓN Y SU CONTEXTO

INSTEL 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 INSTEL 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, INSTEL 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

INSTEL 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.

- 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 nuevas 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: INSTEL 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.

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

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.

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

El alcance definido por INSTEL 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 20 de agosto del 2025."

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

La política del Sistema de Gestión de seguridad de la Información de INSTEL, es una declaración ética, responsable, establecida por la Gerencia General y de cumplimiento en toda la organización, garantiza la adecuada gestión de la seguridad de la información procesada y/o albergada por los sistemas y servicios contemplados en el alcance, con el compromiso de cumplir con los requisitos relacionados con la Seguridad de la Información.

Para desarrollar esta política, la dirección de INSTEL 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.
- 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

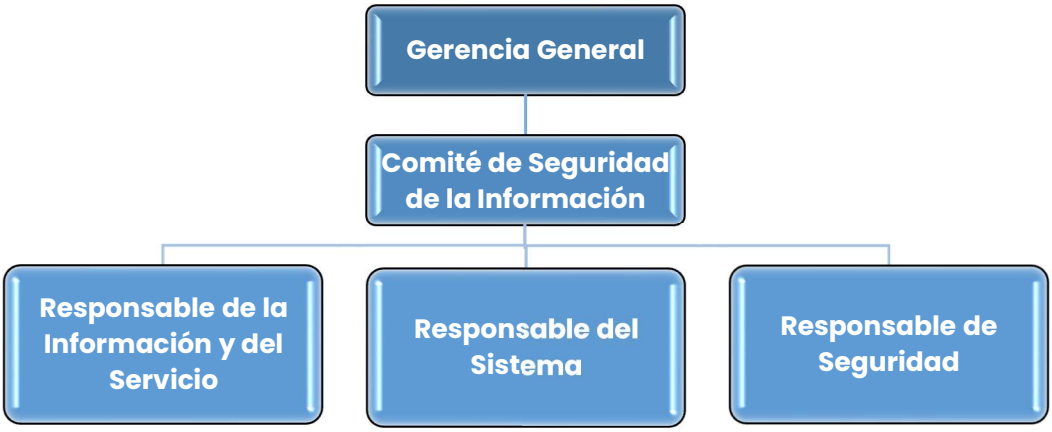
La Gerencia General determina los roles o funciones de seguridad, definiendo para cada uno, los deberes y responsabilidades del cargo, así como el procedimiento para su designación y renovación, el acta del Comité de Seguridad donde se designen nominalmente sus miembros, o las altas y bajas que se puedan llegar a producir.

3.6.1. Organigrama del SGSI

En el Organigrama estructural de la organización todos los cargos dependen de la Dirección Financiera y Operaciones.

El área de IT queda conformada por el Responsable de la Información y el Servicio y el Responsable de Sistemas.

A continuación, se ilustra el organigrama para la Operatividad del Sistema de Gestión de Seguridad de la Información:



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. 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

Identificar, evaluar y tratar los riesgos relacionados con la seguridad de la información, además de los riesgos derivados del cambio climático, implementando controles adecuados para mitigarlos.

La organización ha revisado la metodología de MAGERIT para:

- Identificar y valorar activos.
- Evaluar amenazas y vulnerabilidades.
- Establecer controles y medidas de tratamiento.

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

Esta política será revisada al menos una vez cada dos años o cuando se produzcan cambios significativos en el entorno tecnológico, normativo o del negocio.

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 TRANSFERENCIA, ELIMINACIÓN, DESTRUCCIÓN Y TRATAMIENTO DE LA INFORMACIÓN

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

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.

8.3. POLÍTICA DE GESTIÓN DE LOS 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 DE SEGURIDAD SOBRE EL TALENTO HUMANO

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.

8.5. POLÍTICA DE CAPACITACIÓN Y ENTRENAMIENTO

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.

8.6. 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.
- 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

8.7. POLÍTICA DE SEGURIDAD FÍSICA 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.

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

Todas las redes de computadores, 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.

8.9. POLÍTICA DE SISTEMAS DE RESPALDO Y RECUPERACIÓN

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 una prueba de recuperación de información.

8.10. POLÍTICA DE GESTIÓN DE LOS INCIDENTES DE SEGURIDAD

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.
- Política corporativa estricta de no negociar con atacantes.

8.11. POLÍTICA DE PLANES DE RECUPERACIÓN ANTE DESASTRES

Se debe contar con planes para la recuperación ante desastres documentados, oficializados, divulgados y aprobados, de modo que todo el personal este enterado de las acciones técnicas a realizar en caso de fallo de la red, bases de datos, sistema operativo y aplicaciones en general. Todos los planes de recuperación ante desastres deben tener un análisis de riesgos previo, acorde con la metodología definida por la organización.

8.12. POLÍTICA DE SEGURIDAD DE PROVEEDORES

Debe asegurarse de que los proveedores cumplen con los requisitos de seguridad establecidos en el SGSI, desde la fase de selección hasta la finalización del contrato, incluyendo mecanismos de supervisión y control continuos.

8.13. POLÍTICA DE CUMPLIMIENTO NORMATIVO

Establecer el compromiso de la organización con el cumplimiento de todos los requisitos legales, reglamentarios, contractuales y otros compromisos aplicables relacionados con la seguridad de la información, garantizando la integridad, confidencialidad y disponibilidad de los activos de información.

8.14. POLÍTICA SOBRE LA DOCUMENTACIÓN

Toda la documentación y registros en general deben protegerse acorde a su criticidad:

- Se debe emplear las metodologías para la clasificación de información.
- Si la información es crítica, ésta se debe proteger a través de elementos criptográficos.
- Los registros y documentos digitales deben tener control de acceso.

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. NORMATIVIDAD APLICABLE

- Reglamento General de Protección de Datos (RGPD)

11.1. ESTÁNDARES Y REGULACIONES EXTERNAS

- ISO/IEC 27001 – Sistemas de Gestión de la Seguridad de la Información, Ciberseguridad y Protección de la Privacidad.

12. ANEXOS

- PSIG-031.A01 DECLARACIÓN DE APLICABILIDAD

13. CONTROL DE CAMBIOS

Edición	Fecha	Comentarios
01	16/06/2025	*Creación del documento para el SGSI*
02	7/08/2025	*Cambios en la política y objetivos del SGSI*
03	13/11/2025	*Nuevos objetivos SGSI 2025- 2026*

46349590J ALEJANDRO MARTINEZ (R: B59524272)

Firmado digitalmente por 46349590J ALEJANDRO MARTINEZ (R: B59524272)
Fecha: 2025.11.20 19:25:58 +01'00'