COMPUNETGROUP

POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

Código:	CPN-POL-PSI
Versión:	Versión 7
Fecha de la versión:	20 de marzo de 2026
Creado por:	Oficial de Seguridad de la Información (OSI)
Aprobado por:	Comité de Seguridad de la Información (CSI)
Nivel de confidencialidad:	PÚBLICA

Tabla de contenido

1. Objetivo, alcance y usuarios 3

2. Documentos de referencia 3

3. Terminología 4

4. Roles y Responsabilidades 6

5. Gestión de la Seguridad de la Información 7

6. Política 8

6.1. Requisitos de Seguridad de la Información 8
6.2. Apoyo al Sistema de Gestión de Seguridad de la Información 8
6.3. De la Información Interna y el Uso aceptable de activos 8
6.4. De la Información de Clientes y Socios de Negocio 9
6.5. De las Auditorías 9
6.6. Del Compromiso de Alta Dirección 9
6.7. Deberes de los Colaboradores 10
6.8. Organización de la seguridad de información 10
6.9. Contacto con grupos de interés especial 10
6.10. Control de accesos 10
6.11. Seguridad de las operaciones 11
6.12. Seguridad de las comunicaciones 11
6.13. Adquisición, desarrollo y mantenimiento de sistemas 11
6.14. Gestión de Incidentes de seguridad de la información 12
6.15. Cumplimiento 12
6.16. Concientización, Educación y Formación 12
6.17. Comunicación 12

7. Validez y gestión de documentos 13

8. Difusión 13

1. Objetivo, alcance y usuarios

CompunetGroup SpA es una empresa dedicada a proveer “Soluciones para la Seguridad de la Información y Ciberseguridad” fundada en enero de 1994. Como tal, CompunetGroup reconoce la importancia y valor de la información generada, almacenada, transportada y/o accedido producto inherente de nuestra misión corporativa. A razón de esto, la presente política regula el manejo de información en COMPUNETGROUP definiendo las medidas para el resguardo de la confidencialidad, integridad y disponibilidad de la información propia de CompunetGroup, sus clientes, proveedores y partes interesadas alineada a los requerimientos normativos y legales y alineada al marco de seguridad ISO 27001:2022 mediante la implantación de un Sistema de Gestión de Seguridad de la Información el cual nos permite, como organización, lograr niveles adecuados de seguridad para todos los activos de información relevantes de forma tal de garantizar que los riesgos de seguridad de la información sean conocidos, abordados, gestionados y minimizados de forma documentada, sistemática, repetible, eficiente y con capacidad de adaptación a los nuevas amenazas, desafíos, normativas, leyes, riesgos, entornos y tecnologías. De esta manera, la presente política define los objetivos de seguridad de la información, roles y responsabilidades, las distintas políticas específicas de seguridad de la información y el formato y mantención de políticas, procedimientos, instructivos y protocolos.

2. Documentos de referencia

- Norma Chilena ISO 27001:2022
- Norma Chilena ISO 27002:2022
- Alcance del Sistema de Gestión de Seguridad de la Información
- Metodología de Evaluación de Riesgos
- Declaración de Aplicabilidad
- Plan de Tratamiento de Riesgos
- Informe de Evaluación de Riesgos
- Inventario de Activos
- Requerimientos Legales, Regulatorios y Contractuales
- Política de Control de Acceso
- Política Seguridad con Proveedores
- Procedimientos:
- Operación para Gestión de TI
- Gestión de Incidentes
- Continuidad de Negocio
- Plan de Carrera
- Principios de Ingeniería de Sistemas Seguros

3. Terminología

1. **Activo informático:** toda información almacenada en una red y sistema informático que tenga valor para una persona u organización.

2. **Agencia**: la Agencia Nacional de Ciberseguridad, que se conocerá en forma abreviada como ANCI.

3. **Auditorías de seguridad**: procesos de control destinados a revisar el cumplimiento de las políticas y procedimientos que se derivan del Sistema de Gestión de la Seguridad de la Información.

4. **Autenticación:** propiedad de la información que da cuenta de su origen legítimo.

5. **Ciberataque:** intento de destruir, exponer, alterar, deshabilitar, o exfiltrar u obtener acceso o hacer uso no autorizado de un activo informático.

6. **Ciberseguridad:** preservación de la confidencialidad e integridad de la información y de la disponibilidad y resiliencia de las redes y sistemas informáticos, con el objetivo de proteger a las personas, la sociedad, las organizaciones o las naciones de incidentes de ciberseguridad.

7. **Confidencialidad:** propiedad que consiste en que la información no es accedida o entregada a individuos, entidades o procesos no autorizados.

8. **Disponibilidad:** propiedad que consiste en que la información está disponible y es utilizable cuando es requerida por un individuo, entidad o proceso autorizado.

9. **Equipo de Respuesta a Incidentes de Seguridad Informática o CSIRT**: centros multidisciplinarios que tienen por objeto prevenir, detectar, gestionar y responder a incidentes de ciberseguridad o ciberataques, en forma rápida y efectiva, y que actúan conforme a procedimientos y políticas predefinidas, ayudando a mitigar sus efectos.

10. **Incidente de ciberseguridad**: todo evento que perjudique o comprometa la confidencialidad o integridad de la información, la disponibilidad o resiliencia de las redes y sistemas informáticos, o la autenticación de los procesos ejecutados o implementados en las redes y sistemas informáticos.

11. **Integridad:** propiedad que consiste en que la información no ha sido modificada o destruida sin autorización.

12. **Red y sistema informático:** conjunto de dispositivos, cables, enlaces, enrutadores u otros equipos de comunicaciones o sistemas que almacenen, procesen o transmitan datos digitales.

13. **Resiliencia:** capacidad de las redes y sistemas informáticos para seguir operando luego de un incidente de ciberseguridad, aunque sea en un estado degradado, debilitado o segmentado, y la capacidad de las redes y sistemas informáticos para recuperar sus funciones después de un incidente de ciberseguridad.

14. **Riesgo:** posibilidad de ocurrencia de un incidente de ciberseguridad; la magnitud de un riesgo es cuantificada en términos de la probabilidad de ocurrencia del incidente y del impacto de las consecuencias de este.

15. **Vulnerabilidad:** debilidad de un activo o control que puede ser explotado por una o más amenazas informáticas.

16. **Uso Aceptable:** Todo uso respecto a un activo y/o información en el marco de su diseño y propósito y para quienes poseen acceso a este.

17. **Colaborador:** es toda persona a la cual se le concede autorización para acceder a información y sistemas de COMPUNETGROUP

18. **Responsable de la Información:** es el colaborador a cargo de la información y de los procesos que la manipulan sean estos manuales, mecánicos o electrónicos.

19. **Oficial de Seguridad:** autoridad máxima designada para la definición, diseño, implementación y supervisión de las medidas de seguridad de la información.

20. **Comité de Seguridad:** es el equipo conformado por Director Ejecutivo, Oficial de Seguridad de la Información y Gerentes de Área; Todos, responsables de la toma de decisiones en temas de la seguridad de la información.

21. **Control de Acceso:** Medios para asegurar que el acceso a los activos está autorizado y restringido en función de los requisitos de negocio y de seguridad.

22. **Información:** La información es la interpretación que se da a un conjunto de datos, pudiendo residir está en medios electromagnéticos, físicos o en el conocimiento de las personas. En el caso de la presente política, se entenderá como información a toda forma proveniente de datos relacionados con los procesos de negocio CompunetGroup, así como antecedentes proporcionados tanto por colaboradores, internos como los externos, siempre que sea dentro del contexto del ejercicio de sus funciones y del cumplimiento de sus obligaciones.

23. **Seguridad de la Información:** Es el nivel de confianza que la organización desea tener de su capacidad para preservar la confidencialidad, integridad y disponibilidad de la información. Su propósito es proteger la información de amenazas, con el fin de asegurar la continuidad del negocio, minimizar el daño y, cumplir su misión y objetivos estratégicos.

24. **Información Pública:** Toda aquella información no catalogada como secreta o confidencial.

25. **Información reservada:** toda aquella información la cual debe tener acceso personas explícitamente definidos e identificados y/o información que debe ser tratada de manera reservada.

26. **Información Secreta:** toda aquella información cuyo conocimiento está circunscrito a las

autoridades o personas a las que vayan dirigidos.

4. Roles y Responsabilidades

Alta Gerencia: Será responsable de conocer los objetivos de seguridad de la información, velar por el cumplimiento de estos y disponer los recursos necesarios para su cumplimiento.

Director Ejecutivo: En su calidad de tal, responde ante el Directorio por la existencia y cumplimiento de las medidas que mantengan un nivel de seguridad de la información conforme los objetivos y alineados a las disposiciones legales y regulatorias.

Oficial de Seguridad: Máxima autoridad en el Sistema de Gestión de Seguridad de la Información de CompunetGroup. Principal responsable en la definición, implementación y supervisión de los criterios de seguridad de la información, para lo cual deberá analizar periódicamente el nivel de riesgo existente, asesorando en sus soluciones. Deberá definir normas y validar todo procedimiento de las áreas de negocios para garantizar y proteger los activos de la información. Una vez autorizada la implementación de las medidas, deberá coordinar con quienes corresponda su materialización oportuna y correcta. Responsable de evaluar y medir el cumplimiento del SGSI de los colaboradores de la organización y también de la eficiencia del sistema de gestión.

Comité de Seguridad: Máximo responsable de entregar las directrices para conformar la Política de Seguridad de la Información. Debe evaluar el estado del sistema de gestión, su nivel de madurez, riesgos y planes de mitigación. Responsable de identificar todos los objetivos y estrategias del SGSI, dirigir, controlar y aprobar los planes de acción relacionados con la seguridad de la información.

El comité está integrado por: Oficial de Seguridad, Gerente general, Gerente de Ciberseguridad, Gerente Comercial, Gerente de Desarrollo, responsable de Administración y Finanzas, Jefe de Servicios

Comité de Contingencia: Entidad responsable de, en caso de contingencia: planificar, coordinar, unificar puntos de vista y tomar líneas de acción de todas las áreas de la Empresa que tienen relación con la contingencia.

Esta entidad está conformada por los mismos miembros del Comité de Seguridad

Colaboradores: responsables de cumplir con lo formalizado en este documento y aplicarlo en su entorno diario. Poseen la obligación de alertar de forma oportuna y adecuada cualquier incidente que atente contra la seguridad de la información.

Jefe de Servicios: Aplicar las políticas, procesos y procedimientos definidos para Seguridad de la Información, asegurar disponibilidad de los recursos para que se del cumplimiento a estos.

Responsable de Administración y Finanzas: Aplicar las políticas, procesos y procedimientos definidos para Seguridad de la Información, garantizar el resguardo de la Confidencialidad de la información crítica del negocio bajo su responsabilidad.

5. Gestión de la Seguridad de la Información

CompunetGroup ha definido los siguientes objetivos generales de seguridad de la información:

- Proteger la información de CompunetGroup, sus colaboradores, clientes, proveedores, socios y partes interesadas durante todo el ciclo de vida de la información.
- Concientizar y Capacitar a todos los miembros y colaboradores de CompunetGroup en el resguardo y garantía de la integridad, confidencialidad y disponibilidad de la información.
- Implementar la mejora continua en todos nuestros procesos y procedimientos mejorando continuamente nuestra postura de seguridad de la información.

Para dar cumplimiento a los objetivos definidos, se identificarán todos los activos de información involucrados en los distintos procesos de negocios y procesos de soporte identificando al dueño de cada proceso y activo, las vulnerabilidades y amenazas de cada proceso y activo de información y, en función del impacto, determinar el riesgo existente, siempre bajo el alcance del sistema de gestión y, cuando aplica, a toda la organización de forma transversal. Con la información anterior, se aplicarán los controles necesarios que nos permitan gestionar debidamente el riesgo. CompunetGroup medirá el cumplimiento de todos los objetivos. El Oficial de Seguridad de la Información es el responsable de definir el método para medir el cumplimiento de los objetivos; la medición se realizará al menos al menos una vez al año y el Oficial de Seguridad de la Información analizará y evaluará los resultados y los reportará a alta dirección como material para la revisión por la Dirección. Oficial de Seguridad de la Información es responsable de registrar los detalles sobre los métodos de medición, periodicidades y resultados en el Informe de Medición.

6. Política

6.1. Requisitos de Seguridad de la Información

- La presente Política, y todo el SGSI, deben cumplir los requisitos legales y normativos importantes para la organización en el ámbito de la seguridad de la información, como también con las obligaciones contractuales.

6.2. Apoyo al Sistema de Gestión de Seguridad de la Información

- A través del presente, la Alta Dirección de CompunetGroup declara que en la implementación y mejora continua del SGSI se contará con el apoyo de los recursos adecuados para lograr todos los objetivos establecidos en esta Política, como también para cumplir con todos los requisitos identificados.
- Se deberá garantizar la revisión periódica de las políticas de seguridad (al menos una vez por año calendario), así como garantizar la existencia de mecanismos de difusión y educación en CompunetGroup.

6.3. De la Información Interna y el Uso aceptable de activos

- La información es un activo vital y todos sus accesos, usos y procesamiento, deberán ser consistentes con las políticas y estándares emitidos por CompunetGroup en cada ámbito en particular.
- La información debe ser protegida, por sus responsables, de una manera consistente con su importancia, valor y criticidad, siguiendo las reglas establecidas en las políticas específicas de seguridad de la información, sus procedimientos asociados y en las recomendaciones dadas por el responsable designado de dicha información.
- Toda la información creada o procesada por CompunetGroup debe ser considerada como “Confidencial”, a menos que se determine otro nivel de clasificación, pudiendo ser “Secreto” o “Publico”. Periódicamente se deberá revisar la clasificación, con el propósito de mantenerla o modificarla según se estime apropiado.
- Los activos de información asignados o a los cuales se posee acceso deben ser empleados únicamente para la función y propósito inherente en el proceso en que estos existen. Cualquier otro uso es considerado “uso no aceptable” y será abordado conforme al impacto de este en términos de sanciones, normativo y/o legal de ser necesario.
- Se deberá considerar la existencia de un inventario y responsables de activos de información tecnológicos (aplicaciones e infraestructura) o no tecnológicos, así como procesos para mantenerlos.
- Se deberá considerar una definición y caracterización para la identificación, priorización y

clasificación de los activos con el objetivo de proteger su confidencialidad, integridad y disponibilidad.

- Se deberá considerar una metodología para la gestión de la seguridad dedicada para los activos expuestos al ciberespacio.

6.4. De la Información de Clientes y Socios de Negocio

- Dada la naturaleza de los servicios que CompunetGroup provee, se compromete a asegurar que la información obtenida no será divulgada sin previa autorización y estará protegida de igual manera que la información interna.
- El compartir información de clientes y/o socios de negocio con terceros, únicamente se dará bajo un contexto legal y en el marco de una orden judicial.

6.5. De las Auditorías

- Con el fin de velar por el correcto uso de los activos de información de su propiedad, CompunetGroup se reserva el derecho de auditar en todo momento y sin previo aviso, el cumplimiento de las políticas vigentes y que dicen relación con el acceso y uso que los usuarios hacen de los activos de información.
- CompunetGroup se reserva el derecho de tomar medidas administrativas y/o judiciales en contra el o los colaboradores que no den cumplimiento a lo dispuesto en la presente política, las políticas específicas que se deriven de esta y en su documentación de referencia, acciones que pueden ser solicitadas por su jefatura directa, el Oficial de Seguridad de la Información, el responsable de Recursos Humanos o el Director Ejecutivo.

6.6. Del Compromiso de Alta Dirección

- La Alta Dirección velará por la existencia de un plan formal de difusión de esta política y las políticas específicas que la sustenten.
- La Alta Dirección procurará que todos los colaboradores sean concientizados y reciban entrenamiento en materia de seguridad, consistente con sus necesidades y su rol en CompunetGroup.
- La Alta Dirección propiciará la existencia de mecanismos o procedimientos formales que permitan asegurar la continuidad del negocio ante situaciones que impidan el acceso a la información imprescindible para el funcionamiento de la organización.

6.7. Deberes de los Colaboradores

- La información y las tecnologías de información deben ser usadas sólo para propósitos relacionados su rol y labor en CompunetGroup debiéndose aplicar criterios de buen uso en su utilización.
- Las claves de acceso a la información y a las tecnologías de información son individuales, intransferibles y de responsabilidad única de su propietario.
- El personal está en la obligación de alertar, de manera oportuna y adecuada, cualquier incidente que atente contra lo establecido en esta política.
- Está absolutamente prohibido a los colaboradores de CompunetGroup, divulgar cualquier información que esté catalogada como “Confidencial” o “Secreta”.

6.8. Organización de la seguridad de información

- Se deberán definir las responsabilidades específicas en materia de seguridad de la información de las diferentes unidades internas, considerando: la responsabilidad de las unidades de negocios en relación con el cumplimiento de las políticas y normas de seguridad.

6.9. Contacto con grupos de interés especial

CompunetGroup declara una actitud activa de vigilancia permanente respecto a Seguridad de la Información y Ciberseguridad, es por esto por lo que considera el contacto con grupos de interés especial en estas materias, como, por ejemplo:

- CSIRT gubernamental de Chile
- Comunidades y Foros de Seguridad y Ciberseguridad local e internacional
- Forma parte de la comunidad ciberseguridad, estando suscrito a boletines de seguridad de la información y ciberseguridad para recibir alertas y alarmas respecto de amenazas y vulnerabilidades

6.10. Control de accesos

Se deberán establecer procesos y requisitos en relación con:

- Establecer las responsabilidades del usuario en relación con el uso de claves y de sus dispositivos electrónicos (estación de trabajo, notebook u otro asignado).
- Gestión de accesos de usuario que establezca procedimientos para la identificación, asignación y revisión de privilegios.
- Control de acceso a redes considerando la segregación de las redes y la limitación de la

conectividad de red al máximo posible.

- Control de acceso a los sistemas operativos considerando estándares para la definición y mantención de claves.
- Control de acceso a las aplicaciones e información considerando el perfilado de dichos accesos.
- Controles de movilidad y teletrabajo.

6.11. Seguridad de las operaciones

Se deberán establecer requisitos con respecto a lo menos:

- La operación tecnológica debe incorporar una correcta segregación de funciones entre los ambientes de desarrollo, prueba (QA) y producción.
- Controles de seguridad contra software malicioso.
- Controles para el uso de medios de almacenamiento.
- Solo se permitirá la descarga, instalación y/o ejecución de software autorizado.
- Monitoreo y auditoría de las actividades realizadas sobre la red y sobre los sistemas.

6.12. Seguridad de las comunicaciones

Se deberán establecer requisitos con respecto a lo menos:

- Controles de seguridad con respecto a las redes de comunicación (firewall, firewalls aplicativos, IPS (sistemas de prevención de intrusos), entre otros.
- Controles para el acceso de terceros autorizados a la red.
- Controles para la realización de servicios de comercio electrónico.
- Monitoreo y auditoría de las actividades realizadas sobre la red y sobre los sistemas.

6.13. Adquisición, desarrollo y mantenimiento de sistemas

Se deberán considerar, para el desarrollo y mantenimiento de sistemas participación y/o requerimientos de seguridad, en particular para aplicaciones del tipo web, que aseguren aspectos tales como el correcto procesamiento en las aplicaciones, la aplicación de controles criptográficos (cuando aplique), la seguridad de los archivos de sistemas, la seguridad durante el proceso de desarrollo y soporte. Adicionalmente y de acuerdo con la criticidad de los servicios, se deberán realizar pruebas tendientes a identificar las potenciales vulnerabilidades en servidores, aplicaciones y contenidos asociados.

6.14. Gestión de Incidentes de seguridad de la información

Se deberá mantener registro de incidentes, eventos y vulnerabilidades. Adicionalmente deberán estar definidos los procesos y equipos de respuesta a un evento de seguridad, así como para el análisis forense de los incidentes de seguridad relevantes tendientes a identificar la causa raíz y establecer planes de acción en los casos que sea necesario Se deberán considerar pruebas ante amenazas de Seguridad de la Información y Ciberseguridad.

6.15. Cumplimiento

Todas las unidades de CompunetGroup son responsables del cumplimiento de esta política. La Alta Dirección, a través del Comité de Seguridad revisará periódicamente (al menos una vez por año) las prácticas de seguridad de la información, en relación con el cumplimiento de la presente política y sus objetivos.

6.16. Concientización, Educación y Formación

CompunetGroup es responsable de generar y proveer la toma de conciencia a través de la difusión de las políticas, procesos y procedimientos de seguridad de la información de manera tal de garantizar que los colaboradores contribuyen a la eficacia del SGSI beneficiando el desempeño del sistema dando, específicamente, cumplimiento a:

i. Sensibilización a los colaboradores COMPUNETGROUP sobre los resguardos en sus procesos y procedimientos
ii. Aprender cómo comportarse (conciencia) en general con la correcta interpretación de la Política de seguridad, los aportes de personal a la eficacia del SGSI y las implicancias que contrae no cumplir con los requisitos, así como también el uso de la internet y las herramientas derivadas de ellas
iii. Promover las mejores prácticas y pautas entre los colaboradores COMPUNETGROUP
iv. Garantizar que los procesos y procedimientos están disponibles para quien y cuando los necesite y que estos son medidos y mejorados.

6.17. Comunicación

CompunetGroup ha establecido un plan de comunicaciones, interna y externa, pertinentes al sistema de gestión de seguridad de la información señalando, debidamente y cuando corresponde; que comunicar, cuando comunicar, a quien comunicar y como comunicar.

7. Validez y gestión de documentos

Este documento es válido de forma indefinida o hasta que una versión posterior lo reemplace.

El propietario de este documento es el Comité de Seguridad de la Información, que debe verificar, y si es necesario actualizar, el documento por lo menos una vez al año.

Al evaluar la efectividad y adecuación de este documento, es necesario tener en cuenta los siguientes criterios:

- Cantidad de colaboradores y participantes externos que cumplen una función en el SGSI y que no están familiarizados con el presente documento.
- No cumplimiento del SGSI con las leyes y normas, las obligaciones contractuales y con los demás documentos internos de la organización.
- Ineficacia de la implementación y mantenimiento del SGSI.
- Responsabilidades ambiguas para la implementación del SGSI.

8. Difusión

Se debe difundir la política fijada por este instrumento a través de e-mail y/o intranet institucional a los(as) colaboradores(as) de CompunetGroup, una vez al año. Resulta clave para que la presente política se integre en la cultura organizacional, la existencia de un plan formal de difusión, capacitación y sensibilización en torno a la seguridad de la información. El Oficial de Seguridad de la información es el responsable de la ejecución del plan y el cumplimiento de sus objetivos, así como la existencia de un plan comunicacional que lo complemente.

I. **Establézcase** la obligación de el/la Oficial de Seguridad de la Información de CompunetGroup de difundir la política fijada por este instrumento a través de e-mail y/o intranet corporativo.

ANÓTESE, COMUNÍQUESE, CÚMPLASE Y ARCHÍVESE

CÉSAR MILLAVIL ARENAS

Director Ejecutivo
CompunetGroup

Santiago, 01 de marzo 2024.

DISTRIBUCIÓN:

- Gerente de Servicios
- Oficial de Seguridad
- Comité de Seguridad de la Información
- Colaboradores
- Socios de Negocio
- Partes Interesadas

Historial de modificaciones

Fecha	Versión	Creado por	Descripción de la modificación
10-01-2023	6.0	MLT	Se actualiza versión de la Política General de Seguridad de la Información
25-04-2023	6.1	GG-OSI	Revisión y actualización de documento.
01-03-2024	6.2	OSI	Revisión y actualización de definiciones del documento con relación a la ley marco sobre ciberseguridad e infraestructura crítica de la información.
20-03-2026	7	OSI	Integracion con SGC

CompuNet®