POL-01 – SEGURIDAD DE LA INFORMACIÓN

Versión 1.0

Junio 2025

Control de Cambios

Fecha	Versión	Tema	Elaborado por	Revisado por	Principales cambios
09/06/2025	1.0	Seguridad de la información	Oficial de Seguridad	Equipo SGI	● Creación

Contenido

1. Objetivo

Establecer los principios, lineamientos y responsabilidades que permitan proteger de manera eficaz la confidencialidad, integridad y disponibilidad de la información gestionada por la organización, garantizando el cumplimiento de los requisitos legales, contractuales y normativos aplicables. Esta política busca definir un marco de referencia para la implementación, mantenimiento y mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI), asegurando que todas las funciones relacionadas con la seguridad estén claramente asignadas, documentadas y segregadas cuando corresponda, con el fin de minimizar los riesgos derivados de accesos no autorizados, errores operativos o conflictos de interés.

2. Alcance

Esta política aplica a todos los colaboradores, contratistas, practicantes y terceros que trabajen en las instalaciones físicas o remotas de Verity, y que tengan acceso a información confidencial o sistemas informáticos de la organización.

3. Referencias Normativas

La presente política se define considerando las recomendaciones de la siguiente normativa:

- Norma ISO/IEC 27001:2022, Seguridad de la Información, ciberseguridad y protección de la privacidad. Sistema de gestión de la seguridad de la información.

  Requisito: Control A.5.1. Políticas para la seguridad de la información.
  Requisito: Control A.5.2. Funciones y responsabilidades de seguridad de la información.
  Requisito: Control A.5.3. Segregación de funciones.
  Requisito: Control A.5.4. Responsabilidades de la dirección.
  Requisito: Control A.5.5. Contacto con autoridades.
  Requisito: Control A.5.6. Contacto con grupos de interés especiales.
  Requisito: Control A.5.8. Seguridad de la información en la gestión de proyectos.

4. Definiciones

Activo de Información: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de esta (*sistemas, soportes, edificios, personas, etc.*) que tenga valor para la organización.

Seguridad de la Información: Preservación de la confidencialidad, integridad y disponibilidad de la información.

Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

Disponibilidad: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

Integridad: Propiedad de la información relativa a su exactitud y completitud.

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.

Amenaza: Cualquier causa potencial de un incidente no deseado que puede provocar daño a un activo de información, a los procesos del negocio o a la organización.

Vulnerabilidad: Es una debilidad de un activo informático, o sistema de información que puede ser explotada por una o más amenazas para causar un daño. Las debilidades pueden aparecer en cualquiera de los elementos de una computadora, tanto en el hardware, el sistema operativo, cómo en el software.

5. Descripción de la Política

La presente política es parte integral de la documentación del Sistema de Gestión de Seguridad de la Información (SGSI) y tiene como objetivo establecer los lineamientos y responsabilidades para proteger la confidencialidad, integridad y disponibilidad de la información de la organización, asegurando una gestión segura, con funciones claramente definidas y segregadas, conforme a los requisitos legales, contractuales y normativos aplicables.

5.1 ANTECEDENTES GENERALES

Verity está comprometida con la Gestión de la Seguridad de Información y Ciberseguridad en todos sus aspectos, impulsando una cultura de protección de la información, a fin de asegurar la confidencialidad, integridad y disponibilidad de la información propia y de terceros, cumpliendo el marco normativo y legal, lo cual es gestionado mediante el sistema de gestión de Seguridad de la Información.

Verity diseña y ejecuta estrategias para prevenir, controlar y reducir riesgos que puedan afectar la operación de la organización, por ende, los intereses de sus clientes. Además, reconoce que la información es uno de los activos más importantes para cumplir las funciones y objetivos que han sido definidos por la compañía, de ahí la importancia de realizar un análisis del contexto interno y externo de la entidad, con relación a seguridad de la información, para identificar cuáles son los riesgos que pueden o afectan su capacidad para lograr los resultados esperados frente al SGSI; así como identificar cuáles son las necesidades y expectativas de las parte interesadas.

Verity evaluará de forma permanente el contexto externo e interno de la organización dentro del modelo de gestión y presentando al menos de forma anual el análisis del contexto en el directorio de la organización. El análisis del contexto interno y externo deberá contar con instancias para identificar, evaluar y tratar los riesgos de forma oportuna, usando planes de tratamientos establecidos en la metodología de la gestión de la seguridad de información y ciberseguridad. Se establece que para efectos del contexto interno se deben considerar, aspectos administrativos, de comercialización, de recursos humanos, operacionales, financieros, de investigación, culturales y tecnológicos entre otros. Para efectos del contexto externo se deben considerar, aspectos políticos, sociales, tecnológicos, legales, ambientales y sanitarios, entre otros.

5.2 FUNCIONES Y RESPONSABILIDAD DE SEGURIDAD DE LA INFORMACIÓN

La correcta asignación de funciones y responsabilidades es fundamental para garantizar una gestión eficaz de la seguridad de la información. Esta sección establece los roles clave dentro de la organización y define sus responsabilidades en relación con la protección de los activos de información, promoviendo la rendición de cuentas, la trazabilidad y la mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI).

A. Comité de Seguridad

Es el principal órgano de gobierno en materia de seguridad y gestión de riesgos. Será liderado por el Oficial de Seguridad e integrado por representantes de las áreas críticas de la organización, en los términos que establezca su estatuto de funcionamiento. Este organismo responde ante la Dirección, por la existencia y cumplimiento de las medidas orientadas a mantener un nivel de seguridad de la información acorde con las necesidades de Verity.

Su principal función será atender, gestionar y fortalecer el ambiente de control de seguridad de Verity, garantizando que el mismo sea congruente con el contexto y con los objetivos estratégicos de la organización, para lo que deberá:

- Revisar y aprobar la estrategia y políticas de seguridad de la información.
- Definir los criterios y parámetros para la gestión de riesgos de seguridad de la información, incluyendo niveles de aceptación del riesgo.
- Supervisar la implementación de medidas para mitigación de riesgos, planes de contingencia y respuesta ante incidentes de seguridad de la información.
- Implementar planes y programas de concientización y capacitación en seguridad de la información y gestión de riesgos.
- Velar por la disponibilidad de recursos necesarios para materializar los objetivos estratégicos de seguridad de la información.
- Monitorear y evaluar la efectividad del Sistema de Gestión de Seguridad de la Información e identificar oportunidades de mejora.
- Reportar al Director.
- Ejecutar las demás funciones que establezca su estatuto de funcionamiento.

B. Oficial de Seguridad

Profesional con suficiente jerarquía organizacional para liderar, coordinar y supervisar la implementación, mantención y mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI) en las diversas áreas de Verity. Le corresponde proporcionar el juicio experto que orientará la toma de decisiones en la materia dentro de la organización.

Su rol es clave para asegurar que se establezcan medidas de protección eficaces sobre los activos de información, en coherencia con los objetivos estratégicos del negocio, los riesgos identificados y las obligaciones legales y contractuales vigentes. Será responsable de:

- Proponer al Comité de Seguridad la estrategia, políticas, procedimientos y controles de seguridad de la información, velando por su actualización, difusión y cumplimiento.

- Mantener un nivel adecuado de protección de la información de la compañía, orientando la gestión a cumplir los objetivos de integridad, confidencialidad y disponibilidad de la Información.

- Soporte (con su equipo) a las áreas de Verity en la identificación de riesgos claves y mejoramiento de procesos, así como en la mitigación de riesgos según las mejores prácticas de seguridad del mercado, la normativa vigente y siguiendo las bases de los requerimientos de la compañía.

- Coordinar el proceso de evaluación y tratamiento de riesgos.

- Coordinar el levantamiento del inventario de activos de información, velar por su actualización y ser su custodio.

- Documentar la declaratoria de aplicabilidad de controles para tratamiento de riesgos.

- Realizar un monitoreo de cumplimiento de la política de Seguridad basado en la información que arrojan los controles de seguridad de esta política.

- Monitorear la efectividad del Sistema de Gestión de Seguridad de la Información, proponiendo acciones de mejora.

- Coordinar la elaboración de planes de continuidad de negocio y monitorear su implementación y prueba.

- Implementar un plan de concientización y promover una cultura de seguridad de la información dentro de la organización.

- Garantizar la gestión de incidentes de seguridad de la información y coordinar acciones preventivas.

-

- Mantener contacto con autoridades y entidades externas que pudieran prestar apoyo ante incidentes de seguridad o proporcionar información sobre el entorno, nuevas amenazas y buenas prácticas.

  Proponer planes de acción para corregir no conformidades y supervisar su implementación.

C. Colaboradores de Verity

Los colaboradores deberán dar estricto cumplimiento a las directrices establecidas en la presente política y los procedimientos establecidos sobre esta materia, entendiendo que es el principal actor, responsable y motor en la prevención de incidentes de seguridad, que puedan afectar el normal desenvolvimiento de la organización. Serán responsables de:

- Cumplir las políticas de seguridad y hacer un adecuado uso de los activos de información.

- Informar al Oficial de Seguridad y a las jefaturas correspondientes la violación a las políticas de seguridad de la información por parte de otros colaboradores de la organización.

- Reportar a través de los canales que establezca la organización, de manera oportuna, incidentes que pudieran comprometer los activos de información.

- Participar en las capacitaciones de seguridad de la información promovidas por la organización.

D. Dirección

Es responsable directo de establecer el liderazgo estratégico del Sistema de Gestión de Seguridad de la Información (SGSI), asegurando su integración con los objetivos institucionales y el cumplimiento de los principios de confidencialidad, integridad y disponibilidad de la información. Su compromiso es fundamental para garantizar la efectividad del SGSI, el cumplimiento normativo y la mejora continua. Será responsable de:

- Aprobar la Política de Seguridad de la Información y Ciberseguridad y sus modificaciones para asegurar que la organización vele porque exista una adecuada

- gestión del riesgo de seguridad de la información y por el cumplimiento de los requisitos de los grupos de interés.

- Demostrar liderazgo y compromiso activo con el SGSI, promoviendo una cultura organizacional enfocada en la gestión de riesgos y la protección de los activos de información.

  Asignar los recursos necesarios (humanos, financieros, tecnológicos) para la implementación y mejora continua del SGSI.

- Patrocinar y participar en el Comité de Seguridad, guiando las decisiones clave desde una perspectiva institucional.

- Apoyar a las áreas responsables del SGSI (como el Oficial de Seguridad y el Coordinador del SGI) en la toma de decisiones estratégicas y resolución de obstáculos organizacionales.

E. Coordinador del Sistema de Gestión Integrado

Responsable operativo de apoyar la implementación, mantenimiento y mejora continua del Sistema de Gestión de Seguridad de la Información, en estrecha colaboración con el Oficial de Seguridad y otras áreas clave. Su función es asegurar que los procesos definidos en el SGSI se apliquen de forma eficaz, oportuna y documentada, promoviendo la cultura de seguridad en toda la organización. Será responsable de:

- Apoyar la ejecución del SGSI, asegurando el cumplimiento de los controles, políticas y procedimientos establecidos.

- Coordinar actividades operativas del SGSI, como evaluaciones de riesgo, revisiones de controles, gestión documental, planes de tratamiento y seguimiento de no conformidades.

- Colaborar en la identificación, evaluación y actualización de riesgos, asegurando el uso de metodologías y criterios definidos por la organización.
- Gestionar la documentación del SGSI, incluyendo el control de versiones, publicación y accesibilidad para los usuarios.

-
- Mantener una comunicación fluida con el Oficial de Seguridad, informando avances, dificultades y oportunidades de mejora del SGSI.

F. Gerencias

Cumplen un rol estratégico en la implementación y sostenibilidad del Sistema de Gestión de Seguridad de la Información (SGSI). Como líderes de sus respectivas áreas, son

responsables de promover la cultura de seguridad, garantizar el cumplimiento de las políticas institucionales y asegurar la correcta aplicación de los controles de seguridad dentro de sus equipos. Será responsable de:

- Identificar los requerimientos legales, normativos y contractuales en materia de seguridad de la información que sean aplicables a sus procesos y supervisar su cumplimiento.

- Gestionar los recursos necesarios para cumplir con los objetivos del sistema. Promover el cumplimiento de la Política de Seguridad de la Información dentro de su área de responsabilidad, asegurando su correcta comprensión y aplicación por parte de los colaboradores.

- Asignar y garantizar la disponibilidad de recursos humanos, tecnológicos y financieros necesarios para implementar y mantener los controles de seguridad aplicables a su área.

- Fomentar la participación de sus equipos en capacitaciones y actividades de concienciación, fortaleciendo el comportamiento seguro en el uso de la información.

- Supervisar la elaboración de planes de continuidad para los procesos de su área.

G. Auditor de la Seguridad de la Información

Verity auditará una vez al año el funcionamiento del Sistema de Gestión de Seguridad de la Información, verificando el nivel de cumplimiento de leyes, normas, políticas, acuerdos y procedimientos aplicables a la seguridad de la información. Será responsable de:

- Planificar, definir los objetivos y dirigir todas las actividades de la auditoría.

- Llevar a cabo de acuerdo con la planificación las reuniones de relevamiento de información con el personal involucrado, para corroborar o extender sus indagaciones.

- Mantener imparcialidad, un lenguaje adecuado, objetividad y ser independiente del área o proceso comprendido dentro del alcance de la auditoría, no auditar su propio trabajo.

- Desarrollar el trabajo de auditoría, revisando la implementación de controles de seguridad de la información, recolectando evidencias, analizando información,

documentación y reportando en el informe de auditoría situaciones de debilidad, para su mejora y eficacia.

5.3 SEGREGACIÓN DE FUNCIONES

Esta política es administrada por el modelo de Gobierno Corporativo asumido por esta Organización, donde cada línea de defensa tiene funciones y responsabilidades específicas y trabajan en estrecha colaboración para identificar, evaluar y mitigar los riesgos de seguridad de la información y ciberseguridad respecto de los objetivos de negocio y las operaciones de Verity. Considerando lo anterior, las funciones y responsabilidades para cada línea de defensa se entenderán de la siguiente manera:

1era Línea de Defensa: Posee y gestiona los riesgos de seguridad de la información y ciberseguridad, a la vez que desarrolla, implementa y ejecuta diariamente los controles definidos para abordar las deficiencias de control y mitigar los riesgos de seguridad de la información y ciberseguridad, a su vez asumen las consecuencias de las afectaciones ocasionadas por los riesgos que sean materializados.

2da Línea de Defensa: Ayuda a formular las estrategias, políticas y estructuras organizacionales que permitan administrar los riesgos de seguridad de la información y ciberseguridad. Realiza actividades de monitoreo. Identifica, en conjunto con la 1ra línea de defensa, las necesidades, regulaciones y políticas aplicables. Identifica y transmite las leyes, regulaciones y normas emitidas en materia de seguridad de la información y ciberseguridad, y monitorea su cumplimiento.

3ra Línea de Defensa: Auditoría Interna (Evaluación del Sistema de Control) proporciona una evaluación independiente del diseño y efectividad de los controles internos sobre los riesgos de seguridad de la información y ciberseguridad, para el desempeño del negocio. Adicionalmente, provee recomendaciones específicas para mejorar el proceso de gestión de seguridad de la información y ciberseguridad, en alineación al Gobierno y Gestión del Riesgo en Verity.

5.4 CONTACTO CON AUTORIDADES Y GRUPOS DE INTERÉS

La organización mantendrá una comunicación formal, estructurada y efectiva con las autoridades competentes y otros grupos de interés relevantes en materia de seguridad de la información, con el objetivo de garantizar el cumplimiento normativo, facilitar la cooperación ante incidentes, y mantenerse informada sobre amenazas emergentes, mejores prácticas y obligaciones regulatorias.

A. Contacto con Autoridades Competentes

La organización establecerá y documentará los canales oficiales de contacto con las autoridades regulatorias, judiciales, administrativas y de seguridad pertinentes, incluyendo, pero no limitándose a:

- Autoridades de protección de datos personales.
- Entidades reguladoras del sector tecnológico y contractual.
- Fuerzas de orden o unidades especializadas en ciberseguridad (cuando aplique). ● Entidades fiscales, tributarias u otras con capacidad de fiscalización.

La respuesta a requerimientos formales, inspecciones o investigaciones será gestionada exclusivamente por las áreas designadas, como la Dirección o el Oficial de Seguridad (CISO).

B. Contacto con Grupos de Interés Especiales

La organización promoverá relaciones con asociaciones, redes de colaboración o comunidades profesionales relacionadas con la ciberseguridad, aseguramiento de calidad, continuidad del negocio y cumplimiento normativo. Esto incluye:

- Grupos de respuesta a incidentes de seguridad, tales como: CSIRT Chile o Alianza Chilena de Ciberseguridad.
- Foros especializados en seguridad de la información y calidad de software. ● Organismos de estandarización, como por ejemplo: ISO ● Asociaciones profesionales y gremios tecnológicos.

La participación en estos grupos permitirá a la organización acceder a alertas tempranas, compartir buenas prácticas, recibir asesoramiento especializado y fortalecer sus capacidades de respuesta frente a amenazas emergentes. En el caso de participar en eventos de interés, tales como: foros de Seguridad, Ciberseguridad y protección de datos, se debe mantener un registro de la participación.

C. Coordinación Interna

Toda comunicación con autoridades o grupos de interés externos deberá ser canalizada, autorizada y registrada por las áreas responsables. Queda estrictamente prohibida la entrega de información institucional a terceros sin la debida validación y trazabilidad. Se asegurará que los responsables mantengan actualizados los datos de contacto institucionales para responder con agilidad en caso de incidentes o requerimientos oficiales.

5.5 SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE PROYECTOS

Incorporar la seguridad como parte integral de la gestión de proyectos permite asegurar el cumplimiento normativo, proteger los activos de información, y garantizar que las soluciones desarrolladas sean consistentes con los lineamientos del Sistema de Gestión de Seguridad de la Información (SGSI) de la organización.

La seguridad de la información debe ser considerada como un componente esencial en la gestión de todos los proyectos desarrollados por la organización, independientemente de su naturaleza, alcance o duración. Esto incluye proyectos internos, proyectos para clientes, iniciativas tecnológicas, de mejora continua, desarrollo de software, implantación de soluciones, o cualquier otro tipo de proyecto que involucre activos de información. Se deben considerar los siguientes elementos:

a) Durante la fase de planificación de los proyectos, se deberán identificar los activos de información que puedan verse afectados, así como los requisitos de confidencialidad, integridad y disponibilidad asociados. Esta evaluación debe permitir la incorporación temprana de controles de seguridad y medidas de mitigación adecuadas al nivel de riesgo identificado.

b) Cada proyecto deberá considerar una evaluación específica de riesgos de seguridad de la información. Esta evaluación incluirá:
   - Identificación de activos de información que se crean, modifican, almacenan o transmiten.
   - Análisis de amenazas, vulnerabilidades y posibles impactos.
   - Propuesta de controles preventivos, detectivos y correctivos necesarios.
   - Revisión y aprobación por parte del Coordinador del SGI o del Oficial de Seguridad.

c) Toda documentación del proyecto (propuestas, contratos, cronogramas, requerimientos funcionales y técnicos, entre otros) deberá incorporar cláusulas o secciones que aseguren el cumplimiento de las políticas de seguridad de la información de la organización y, en su caso, de los requisitos específicos del cliente.

d) Durante la ejecución del proyecto, el cumplimiento de los requisitos de seguridad será monitoreado como parte del control de calidad y gestión de riesgos.

5.6 POLÍTICAS COMPLEMENTARIAS

El Sistema de Gestión de Seguridad de la Información (SGSI) de la organización se sustenta en un conjunto de políticas específicas que, de manera articulada, establecen los principios, lineamientos y controles necesarios para proteger los activos de información, mitigar riesgos y garantizar el cumplimiento de los requisitos legales, normativos y contractuales aplicables.

Estas políticas complementan la presente política general y abordan, de forma detallada, aspectos clave como el control de accesos, la clasificación de la información, la gestión de incidentes, la seguridad física y ambiental, el uso aceptable de recursos tecnológicos, entre otros. A continuación, se enumeran las principales políticas que forman parte integral del SGSI.

- Inteligencia de amenazas
- Gestión de activos
- Transferencia de información
- Control de acceso
- Relación con los proveedores
- Seguridad de la información servicios en la nube
- Gestión de incidentes de seguridad de la información
- Preparación de las TIC para la continuidad del negocio
- Cumplimiento legal y de derechos de propiedad intelectual

- Privacidad y protección de la información de identificación personal (PII)
- Supervisión y estándares operativos
- Trabajo a distancia
- Seguridad física y ambiental
- Escritorio despejado y pantalla limpia
- Seguridad del entorno
- Mantenimiento de equipos
- Dispositivos terminales del usuario
- Controles técnicos operacionales específicos
- Gestión de registros y actividades de seguimiento
- Control de infraestructura y seguridad de redes
- Respaldo de Información
- Uso de criptografía
- Ciclo de vida de desarrollo de sistemas
- Recuperación ante desastres

6. Revisión

La Política de Seguridad de la información será revisada al menos una vez al año, con el fin de asegurar su eficiencia y efectividad, de igual manera será actualizada en caso de que se requiera.

7. Difusión

La totalidad de las políticas deben ser informadas a las Jefaturas para que las difundan según el nivel de acceso permitido a cada colaborador. El mecanismo formal de comunicación es el correo institucional de la organización.

8. Incumplimiento

El incumplimiento de lo establecido en esta política será considerado una falta a los deberes contractuales y normativos del colaborador o tercero. Dicho incumplimiento podrá dar lugar a medidas correctivas, disciplinarias y/o contractuales, conforme a la gravedad del caso, el historial de reincidencia y el impacto potencial o real sobre la seguridad de la información.

Las sanciones aplicables se encuentran descritas en el documento “Política Prevención de Delitos”, el cual forma parte integral del Sistema de Gestión.