

Política General de Seguridad de la Información

1. Declaración Corporativa

VGroup establece y mantiene un Sistema de Gestión de Seguridad de la Información (SGSI) que vela por la seguridad de la información, cumpliendo con los requisitos aplicables y promoviendo la mejora continua del SGSI, destinado a proteger sus activos de información frente a los riesgos y amenazas que puedan afectar su integridad, disponibilidad y/o confidencialidad.

Toda información que gestione VGroup debe ser protegida adecuadamente a través de la implementación de un conjunto de controles, definidos en políticas, normas y procedimientos de seguridad de la información alineados con la norma ISO/IEC 27001:2022.

2. Objetivos

La Política General de Seguridad de la Información tiene como objetivos:

- a) Proteger la confidencialidad y disponibilidad de los activos de propiedad intelectual fabricados por VGroup, especialmente código y material instruccional.
- b) Mantener la confidencialidad de la información de la empresa, especialmente los datos de clientes almacenados en los sistemas de la empresa.
- c) Asegurar la integridad de la información de los sistemas de VGroup, para mantener su correcto funcionamiento.
- d) Asegurar la continuidad de la operación de VGroup, especialmente sus sistemas.

3. Referencias Normativas

La Política General de Seguridad de la Información incorpora y asegura el cumplimiento de los siguientes requisitos normativos y legales aplicables:

- a) Ley 19.628 - Sobre Protección De La Vida Privada.¹
- b) Ley 20.609 - Establece Medidas contra la Discriminación.²
- c) NCh 2728³
- d) ISO/IEC 27001:2022 - Sistemas de gestión de la seguridad de la información.

¹ <https://www.bcn.cl/leychile/navegar?idNorma=141599>

² <https://www.bcn.cl/leychile/navegar?idNorma=1042092>

³ <http://empresas.sence.cl/normacalidad>

4. Alcance

El alcance de lo descrito en esta política está enfocado a los servicios de eLearning y desarrollo de software de la empresa y afecta tanto:

- a) los colaboradores de **VGroup**, proveedores de bienes o servicios; y en general, a todos aquellos con quienes de manera directa o indirecta se establezca alguna relación, contractual o de cooperación con **VGroup**
- b) los activos de información que almacenen, gestionen y/o transporten datos.

5. Responsabilidades y Segregación de tareas

VGroup, representada por su Gerente General, en conjunto con el Comité de Seguridad de la Información, que son los órganos que lideran la organización en el ámbito de la aplicación del SGSI, se comprometen a velar por la fiel y correcta implementación y cumplimiento de esta política y sus requisitos aplicables.

VGroup establece la segregación de tareas como un principio fundamental para reducir el riesgo de errores, fraudes o accesos no autorizados a la información.

Las funciones críticas relacionadas con la seguridad de la información, tales como la administración de accesos, la gestión de cambios, la operación de sistemas, la respuesta a incidentes y la revisión de controles, se encuentran distribuidas entre distintos roles y responsabilidades, de acuerdo con la estructura organizacional y el tamaño de la empresa.

Cuando por razones operativas no sea posible una segregación completa de funciones, se aplicarán controles compensatorios, tales como revisiones periódicas, supervisión por parte del Encargado de Seguridad de la Información o validaciones por la jefatura correspondiente.

Para efectos de la aplicación del Sistema de Gestión de Seguridad de la Información, VGroup identifica como funciones críticas aquellas relacionadas con:

- La administración de accesos y privilegios.
- La gestión de cambios en sistemas y plataformas.
- La evaluación y tratamiento de riesgos.
- La gestión y cierre de incidentes de seguridad.
- La revisión y aprobación de controles del SGSI.

Con el fin de reducir el riesgo de errores, abusos de privilegios o fraudes, **VGroup** procura que las actividades de autorización, ejecución y revisión de dichas funciones no recaigan en una misma persona.

- Las segregaciones específicas por cargo se describen a continuación:

Función crítica	Ejecución	Revisión / Aprobación
Administración de accesos	Área TI / Soporte	Encargado de Seguridad / Jefatura
Gestión de cambios	Área TI / Encargado SGSI	Encargado de Seguridad / Gerencia
Evaluación de riesgos	Encargado de Seguridad	Gerencia General / Comité de Seguridad de la Información
Gestión de incidentes	Área TI / Encargado SGSI	Comité de Seguridad de la Información / Gerencia
Revisión de controles SGSI	Encargado SGSI	Gerencia General

- Las responsabilidades específicas por cargo se describen a continuación:

Cargo	Responsable	Responsabilidades
Gerente General	Macarena Carmona	- Revisar y aprobar la Política General de Seguridad de la Información, considerando los riesgos de seguridad de la información y los cambios relevantes para el SGSI, al menos una vez al año. - Autorizar la provisión de recursos para la correcta implementación de la Política de Seguridad de la Información. - Velar por la implementación del Sistema de Gestión de Seguridad de la Información.
Encargado de Seguridad de la Información	Pablo León	- Realizar un análisis de riesgos de manera anual y actualizar la Política General de Seguridad de la Información con base en sus resultados, cuando corresponda. - Tomar acciones correctivas con base en un proceso de mejora continua. - Ejecutar un plan de mitigación. - Asegurar la capacitación y concientización de las personas. - Establecer un plan de trabajo sobre los resultados de las auditorías internas.
Comité de Seguridad de la Información	Comité de Seguridad de la Información	- Gestionar las respuestas a situaciones de crisis e incidentes. - Realizar ensayos de respuesta frente a situaciones de contingencia mayor.

		- Establecer mecanismos de comunicación de incidentes.
--	--	--

6. Vigencia

Esta política entra en vigencia desde su aprobación formal y se mantiene vigente mientras no sea reemplazada por una nueva versión aprobada.

7. Historial de Revisiones

Esta política debe ser revisada por el Comité de Seguridad de la Información al menos una vez al año y ante cambios significativos en el negocio, la tecnología, la legislación, los riesgos, el personal, la estructura organizacional o ante eventos que ameriten su reevaluación.

Versión	Fecha	Autor	Observaciones
1	13/09/2022	Becyber	Borrador
2	06/11/2022	Pablo León	Revisión
3	01/12/2022	Juan José Cifuentes	Revisión
4	08/12/2022	Macarena Carmona	Aprobación
5	23/01/2023	Juan José Cifuentes	Actualización
6	15/06/2023	Juan José Cifuentes	Actualización
7	09/12/2023	Macarena Carmona	Aprobación
8	10/11/2025	Pablo León	Revisión
9	10/11/2025	Pablo León	Aprobación
10	Pendiente de aprobación	Pablo León	Adaptación a ISO/IEC 27001:2022