1 OBJETIVO

La Política de Seguridad de la Información ("PSI") establece directrices y responsabilidades que orientan el uso aceptable de los activos de información y/o tecnológicos, basándose en los principios de confidencialidad, integridad y disponibilidad de la información.

2 PÚBLICO OBJETIVO

Este documento se aplica a todas las personas (empleados, miembros de Consejos y Comités, directores, pasantes y aprendices) que forman parte de V.tal, así como a las personas de su grupo económico y a todos los terceros que actúan para o representan a V.tal o a cualquier empresa de su grupo económico.

3 DIRECTRICES

3.1 Uso Aceptable de los Recursos de Tecnología de la Información

Los recursos tecnológicos de la empresa, como notebooks, computadoras de escritorio, teléfonos móviles y tablets corporativos, correo electrónico corporativo, internet, redes internas, etc., deben ser utilizados exclusivamente para fines profesionales, en conformidad con los principios éticos y legales. La empresa establece normas para el uso adecuado de sus recursos tecnológicos, que abarcan:

- Responsabilidades individuales y uso ético de los recursos
- Control de accesos e identidad
- Seguridad de infraestructura y dispositivos
- Protección de datos
- Prácticas seguras en el entorno laboral
- Informes de incidentes y comportamientos sospechosos

V.tal realiza un monitoreo continuo de sus recursos tecnológicos, incluyendo servicios de correo electrónico y mensajería, para proteger a la organización, asegurar el cumplimiento de las reglas de esta política y recopilar evidencias de posibles violaciones. La empresa se reserva el derecho de, sin previo aviso, monitorear, interceptar, registrar, examinar, redirigir, retransmitir, copiar o divulgar los datos enviados o recibidos por sus empleados, cuando sea necesario para fines institucionales o investigaciones criminales. Por lo tanto, los empleados deben ser conscientes de que no hay expectativa de privacidad en el uso de estos recursos.

3.2 Gobernanza de la Seguridad de la Información

3.2.1 Políticas y Procedimientos

La PSI y sus normativas deben ser revisadas, aprobadas y divulgadas regularmente, alineadas con los objetivos estratégicos, regulaciones y mejores prácticas.

3.2.2 Comisión Ejecutiva de Seguridad de la Información

La Comisión Ejecutiva de Seguridad de la Información coordina acciones para proteger activos digitales y cumplir objetivos estratégicos, alineando negocios y tecnología con prioridades organizacionales y regulatorias. Debe incluir representantes de todas las vicepresidencias para decisiones integradas y multidisciplinarias.

3.3 Gestión de Riesgos Cibernéticos

La empresa debe adoptar un enfoque estructurado y proactivo para gestionar los riesgos de seguridad de la información, como amenazas cibernéticas, usos indebidos, fraudes y vulnerabilidades, con el objetivo de minimizar impactos financieros, operativos, reputacionales y legales.

3.4 Gestión de Riesgos Cibernéticos en Proveedores

La empresa debe identificar, evaluar y mitigar los riesgos de proveedores, asegurando el cumplimiento de las políticas corporativas, leyes y regulaciones aplicables.

3.5 Gestión de la Continuidad del Negocio

La empresa debe adoptar medidas para garantizar la continuidad de operaciones críticas ante interrupciones, protegiendo procesos, recursos tecnológicos y activos de información, en conformidad con normas regulatorias, buenas prácticas y objetivos estratégicos.

3.6 Gestión de Identidades y Accesos

La empresa debe implementar un programa estructurado para asegurar que solo personas autorizadas accedan a sistemas, datos y recursos, protegiendo activos, reduciendo riesgos y asegurando cumplimiento regulatorio.

3.7 Protección de Datos

La empresa debe adoptar controles para proteger datos de negocios, empleados y clientes, manteniendo las obligaciones de confidencialidad incluso después del desligamiento, según la política vigente.

3.8 Protección Contra Software Malicioso

La empresa debe implementar controles para prevenir, detectar y responder a amenazas relacionadas con software malicioso.

3.9 Seguridad de Aplicaciones

La empresa debe aplicar prácticas de desarrollo seguro en todo el ciclo de vida del software, con controles desde la etapa de planificación, como revisión de código, pruebas, buenas prácticas y análisis automatizados, garantizando la protección de la información.

3.10 Gestión de Vulnerabilidades y Conformidad

La empresa debe identificar y mitigar vulnerabilidades en activos tecnológicos, mediante análisis, pruebas, correcciones oportunas y configuraciones seguras, reduciendo las superficies de ataque.

3.11 Seguridad de Redes, Estaciones de Trabajo y Dispositivos Móviles

La empresa debe implementar controles para proteger redes, estaciones de trabajo y dispositivos móviles contra accesos no autorizados, vulnerabilidades y amenazas.

3.12 Seguridad Física

La empresa debe establecer controles de acceso físico a los entornos de trabajo, procesamiento y almacenamiento de información, exigiendo el uso visible de credenciales por parte de empleados, terceros y visitantes, e implementando controles de protección de instalaciones como suministro eléctrico, climatización e infraestructura de cableado.

3.13 Gestión de Incidentes de Seguridad de la Información

La empresa debe implementar y mantener procesos estructurados para identificar, registrar, analizar y responder a incidentes cibernéticos que puedan causar pérdidas financieras, daños reputacionales o impactos directos e indirectos a la empresa y sus clientes.

Cualquier incidente observado o sospechoso debe ser comunicado inmediatamente al equipo de Seguridad de la Información a través del SOC (Centro de Operaciones de Seguridad), por correo electrónico (vtal-soc@vtal.com) o por teléfono +55 11 5128-8375. Además, cualquier persona que tenga conocimiento o sospecha de cualquier evento que viole las reglas de esta política o normativas complementarias de seguridad de la información puede utilizar el Canal Confidencial para informes anónimos.

3.14 Concienciación en Seguridad

La empresa debe mantener un programa continuo de concienciación en seguridad para educar y capacitar a los empleados en la protección de personas, activos tecnológicos e información, siguiendo las mejores prácticas, normativas regulatorias y la PSI de la empresa, promoviendo una cultura de seguridad integrada en todos los niveles.

3.15 Medidas Disciplinarias y Excepciones

La aceptación formal y el cumplimiento de la PSI son obligatorios para todos los empleados. El incumplimiento puede dar lugar a medidas disciplinarias, como orientaciones, advertencias o despido, conforme a la legislación y normas internas. Las excepciones a las reglas, necesarias para demandas específicas, deben ser presentadas a la gestión de Seguridad de la Información para su análisis y aprobación formal.

3.16 Revisión de la Política

Esta política podrá ser revisada, actualizada y modificada en intervalos planificados o en cualquier momento, a criterio exclusivo de la empresa, siempre que ocurra algún hecho relevante o evento que justifique su revisión.

4 ROLES Y RESPONSIBILIDADES

Consejo de Administración y Alta Dirección

- Aprobar la política y apoyar la estrategia de ciberseguridad alineada con los objetivos organizacionales;
- Designar un director responsable de la política y garantizar los recursos necesarios para su ejecución;
- Monitorear indicadores de seguridad y promover una cultura de protección de la información.

Seguridad de la Información

- Desarrollar y mantener políticas y normas, realizar evaluaciones de riesgos e implementar controles de seguridad;
- Monitorear amenazas, coordinar respuestas a incidentes y conducir análisis post-evento;
- Promover la concienciación, apoyar a las áreas internas, proporcionar informes a la alta dirección y al consejo de administración, y disponibilizar a Anatel el informe sobre la ejecución de la PSI, según lo definido en la resolución o cuando sea solicitado.

Comisión Ejecutiva de Seguridad de la Información

- Evaluar y dar seguimiento a la estrategia de seguridad de la información y priorizar iniciativas basadas en riesgos;
- Acompañar la ejecución de proyectos críticos y la eficacia de los controles implementados;
- Promover la concienciación y el compromiso del liderazgo con los temas de seguridad;
- Tener conocimiento de incidentes de alto impacto y acompañar los planes de respuesta y mitigación;
- Reportar el estado de las iniciativas e indicadores de desempeño al Consejo de Administración, cuando sea aplicable.

Responsables de Área de Negocios

- Garantizar el cumplimiento de las políticas y directrices de seguridad por parte de los empleados, identificar y mitigar riesgos específicos de sus áreas en conjunto con el área de Seguridad de la Información;
- Difundir la cultura de seguridad, participando activamente en entrenamientos y campañas.

Empleados en General

- Conocer y cumplir con las políticas, normas y directrices de Seguridad de la Información;
- Proteger credenciales, contraseñas y otros medios de autenticación, estando prohibido su compartimiento bajo cualquier circunstancia;
- Comunicar inmediatamente incidentes o violaciones al equipo de seguridad;
- Utilizar los recursos de TI de manera autorizada y conforme a las directrices de esta política;
- Registrar una denuncia ante la autoridad competente en caso de pérdida, hurto, robo o extravío de un dispositivo móvil con aplicaciones corporativas configuradas, y posteriormente informar el incidente al equipo de Tecnología, presentando copia del boletín.

5 REFERENCIAS

- ISO/IEC 27001:2022 - Sistemas de Gestión de la Seguridad de la Información - Requisitos
- ISO/IEC 27002:2022 - Controles de Seguridad de la Información
- Ley General de Protección de Datos (LGPD) - Ley n.° 13.709/2018
- Código de Ética y Conducta de V.tal
- Política de Clasificación de Datos
- Política de Continuidad del Negocio
- Política de Controles de Seguridad
- Política de Gestión de Identidades y Accesos
- Política de Gestión de Vulnerabilidades
- Política de Gestión de Riesgos de Seguridad de la Información
- Política de Protección contra Fugas de Información
- Política de Retención de Datos
- Plan de Respuesta y Prevención de Incidentes de Seguridad
- Manual de Privacidad y Protección de Datos Personales para Terceros
- Manual de Ética y Conducta para Terceros
- Marco de Ciberseguridad del NIST: Versión 2.0
- Resolución Anatel n.° 740/2020

6 GLOSARIO

No aplica

7 ANEXOS

No aplica

8 CUADRO DE APROBACIÓN

NOMBRE	CARGO	ÁREA
Sandro Simas	Vicepresidente	Tecnología

APROBADO POR EL CONSEJO DE ADMINISTRACIÓN DE V.TAL EN: 14/05/2025

ESTE DOCUMENTO DEROGA VERSIONES ANTERIORES