

	POLÍTICA	
	Título: Segurança da Informação - Extrato	Código: POL.TEC.POR.001
	Área: Segurança da Informação	Versão: V4.0

1 OBJETIVO

A Política de Segurança da Informação (“PSI”) estabelece diretrizes e responsabilidades que orientam o uso aceitável dos ativos de informação e/ou tecnológicos, baseados nos princípios de confidencialidade, integridade e disponibilidade da informação.

2 PÚBLICO-ALVO

Este documento se aplica a todas as pessoas (colaboradores, membros de Conselhos e Comitês, diretores, estagiários e aprendizes) que integram a V.tal, bem como as pessoas que integram o seu grupo econômico e todos os Terceiros que atuam para ou representam a V.tal – ou qualquer empresa de seu grupo econômico.

3 DIRETRIZES

3.1 Uso Aceitável dos Recursos de Tecnologia da Informação

Os recursos tecnológicos da companhia tais como notebooks, desktops, celulares e tablets corporativos, e-mail corporativo, internet, redes internas etc. devem ser utilizados exclusivamente para fins profissionais, em conformidade com os princípios éticos e legais. A companhia estabelece normas para o uso apropriado de seus recursos tecnológicos que abrangem:

- Responsabilidades Individuais e Uso Ético dos Recursos
- Acessos e Controle de Identidade
- Segurança de Infraestrutura e Dispositivos
- Proteção dos Dados
- Práticas Seguras no Ambiente de Trabalho
- Reporte de Incidentes e Comportamentos Suspeitos

A V.tal realiza monitoramento contínuo de seus recursos tecnológicos, incluindo serviços de e-mail e mensageria, para proteger a organização, assegurar a conformidade com as regras desta política e coletar evidências de possíveis violações. À empresa reserva-se o direito de, sem aviso prévio, monitorar, interceptar, registrar, examinar, redirecionar, retransmitir, copiar ou divulgar dados enviados ou recebidos por seus colaboradores, conforme necessário para fins institucionais ou investigações criminais, de forma os colaboradores devem estar cientes de que não há expectativa de privacidade no uso desses recursos.

	POLÍTICA	
	Título: Segurança da Informação - Extrato	Código: POL.TEC.POR.001
	Área: Segurança da Informação	Versão: V4.0

3.2 Governança de Segurança da Informação

3.2.1 Políticas e Procedimentos

A PSI e seus normativos devem ser revisados, aprovados e divulgados regularmente, alinhados aos objetivos estratégicos, regulações e melhores práticas.

3.2.2 Comissão Executiva de Segurança da Informação

A Comissão Executiva de Segurança da Informação coordena ações para proteger ativos digitais e cumprir objetivos estratégicos, alinhando negócios e tecnologia às prioridades organizacionais e regulatórias. Deve incluir representantes de todas as vice-presidências para decisões integradas e multidisciplinares.

3.3 Gestão de Risco Cibernético

A companhia deve adotar abordagem estruturada e proativa para gerenciar riscos à segurança da informação, como ameaças cibernéticas, uso indevido, fraudes e vulnerabilidades, visando minimizar impactos financeiros, operacionais, reputacionais e legais.

3.4 Gestão de Risco Cibernético em Fornecedores

A companhia deve identificar, avaliar e mitigar riscos de fornecedores, assegurando conformidade com políticas corporativas, leis e regulamentações aplicáveis.

3.5 Gestão de Continuidade de Negócios

A companhia deve adotar medidas para garantir a continuidade de operações críticas em interrupções, protegendo processos, recursos tecnológicos e ativos de informação, alinhada a normas regulatórias, boas práticas e objetivos estratégicos.

3.6 Gestão de Identidade e Acesso

A companhia deve implementar programa estruturado para assegurar que apenas pessoas autorizadas acessem sistemas, dados e recursos, protegendo ativos, reduzindo riscos e garantindo conformidade regulatória.

3.7 Proteção de Dados

A companhia deve adotar controles para proteger dados de negócios, colaboradores e clientes, mantendo obrigações de sigilo mesmo após o desligamento, conforme política vigente.

3.8 Proteção Contra Softwares Maliciosos

A companhia deve implementar controles para prevenir, detectar e responder a ameaças relacionadas a softwares maliciosos.

 O futuro passa por aqui.	POLÍTICA	
	Título: Segurança da Informação - Extrato	Código: POL.TEC.POR.001
	Área: Segurança da Informação	Versão: V4.0

3.9 Segurança de Aplicações

A companhia deve aplicar práticas de desenvolvimento seguro em todo o ciclo do software, com controles desde o planejamento, como revisão de código, testes, boas práticas e escaneamento automatizado, garantindo a proteção das informações.

3.10 Gestão de Vulnerabilidade e Conformidade

A companhia deve identificar e mitigar vulnerabilidades em ativos tecnológicos, com varreduras, testes, correções tempestivas e configurações seguras, reduzindo superfícies de ataque.

3.11 Segurança de Redes, Estações de Trabalho e Smartphones ou Tablets

A companhia deve implementar controles para proteger redes, estações de trabalho e dispositivos móveis contra acessos não autorizados, vulnerabilidades e ameaças.

3.12 Segurança Física

A companhia deve estabelecer controles de acesso físico aos ambientes de trabalho, processamento e armazenamento de informações, exigindo o uso visível de crachá por colaboradores, terceiros e visitantes, e implementando controles de proteção às instalações, como fornecimento elétrico, climatização e infraestrutura de cabeamento.

3.13 Gestão de Incidentes de Segurança da Informação

A companhia deve implementar e manter processos estruturados para identificar, registrar, analisar e responder a incidentes cibernéticos que possam causar prejuízos financeiros, danos reputacionais ou impactos diretos e indiretos à companhia e seus clientes.

Quaisquer incidentes, observado ou suspeito, devem ser comunicados imediatamente para a equipe de Segurança da Informação através do SOC (Security Operation Center) por meio do e-mail (vtal-soc@vtal.com) ou pelo telefone +55 11 5128-8375. Adicionalmente, para qualquer pessoa que tome conhecimento ou suspeite de qualquer acontecimento que viole as regras desta política ou normativos complementares de segurança da informação, está disponível o Canal Confidencial para relatos anônimos.

3.14 Conscientização de Segurança

A companhia deve manter um programa contínuo de conscientização de segurança para educar e treinar colaboradores na proteção de pessoas, ativos tecnológicos e informações, seguindo as melhores práticas, normas regulatórias e a PSI da empresa, promovendo uma cultura de segurança integrada em todos os níveis.

	POLÍTICA	
	Título: Segurança da Informação - Extrato	Código: POL.TEC.POR.001
	Área: Segurança da Informação	Versão: V4.0

3.15 Medidas Disciplinares e Exceções

O aceite formal e cumprimento da PSI é obrigatório para todos os colaboradores. O descumprimento pode resultar em medidas disciplinares, como orientações, advertências ou desligamento, conforme a legislação e normas internas. Exceções às regras, necessárias para demandas específicas, devem ser submetidas à gestão de Segurança da Informação para análise e aprovação formal.

3.16 Revisão da Política

Essa política poderá ser revista, atualizada e alterada em intervalos planejados ou qualquer tempo, a exclusivo critério da companhia, sempre que algum fato relevante ou evento que motive sua revisão.

4 PAPÉIS E RESPONSABILIDADES

Conselho de Administração e Alta Direção

- Aprovar a política e apoiar a estratégia de segurança cibernética alinhada aos objetivos organizacionais;
- Designar um diretor responsável pela política e garantir os recursos necessários para sua execução;
- Monitorar indicadores de segurança e promover uma cultura de proteção da informação.

Segurança da Informação

- Desenvolver e manter políticas e normas, realizar avaliações de riscos e implementar controles de segurança;
- Monitorar ameaças, coordenar respostas a incidentes e conduzir análises pós-eventos;
- Promover conscientização, apoiar áreas internas, prover relatórios à alta direção e ao conselho de administração, além de disponibilizar para a Anatel, relatório sobre a execução da PSI, conforme definido na resolução ou quando solicitado.

Comissão Executiva de Segurança da Informação

- Avaliar e acompanhar a estratégia de segurança da informação e priorizar iniciativas baseadas em riscos;
 - Acompanhar a execução de projetos críticos e a eficácia dos controles implementados;
 - Promover a conscientização e o engajamento das lideranças nos temas de segurança;
 - Ter ciência de incidentes de alto impacto e acompanhar os planos de resposta e mitigação;
- Reportar o status das iniciativas e indicadores de desempenho ao Conselho de Administração, quando aplicável.

 O futuro passa por aqui.	POLÍTICA	
	Título: Segurança da Informação - Extrato	Código: POL.TEC.POR.001
	Área: Segurança da Informação	Versão: V4.0

Gestores de Área

- Garantir a conformidade dos colaboradores com as políticas e diretrizes de segurança, identificar e mitigar riscos específicos de suas áreas em parceria com a área de Segurança da Informação;
- Disseminar a cultura de segurança, participando ativamente de treinamentos e campanhas.

Colaboradores em Geral

- Conhecer e seguir as políticas, normas e diretrizes de Segurança da Informação;
- Proteger credenciais, senhas e outros meios de autenticação, sendo proibido seu compartilhamento sob quaisquer circunstâncias;
- Comunicar incidentes ou violações à equipe de segurança imediatamente;
- Utilizar os recursos de TI de forma autorizada e em conformidade com as diretrizes desta política.
- Registrar boletim de ocorrência junto a autoridade policial no caso de perda, furto, roubo ou extravio de equipamento móvel que tenha aplicativos da companhia configurado e, na sequência, comunicar o incidente à equipe de Tecnologia, apresentando cópia do boletim.

5 REFERÊNCIAS

ISO/IEC 27001:2022: Sistemas de Gestão de Segurança da Informação - Requisitos

ISO/IEC 27002:2022: Controles de Segurança da Informação

Lei Geral de Proteção de Dados (LGPD) - Lei nº 13.709/2018

Código de Ética e Conduta da V.tal

Política de Classificação de Dados

Política de Continuidade de Negócios

Política de Controles de Segurança

Política de Gestão de Identidades e Acessos

Política de Gestão de Vulnerabilidades

Política de Gestão de Risco de Segurança da Informação

Política de Proteção Contra Vazamento de Informações

Política de Retenção de Dados

Plano de Resposta e Prevenção a Incidentes de Segurança

Manual de Privacidade e Proteção de Dados Pessoais para Terceiros

Manual de Ética e Conduta para Terceiros

NIST Cybersecurity Framework: Versão 2.0

Resolução Anatel nº 740/2020

 O futuro passa por aqui.	POLÍTICA	
	Título: Segurança da Informação - Extrato	Código: POL.TEC.POR.001
	Área: Segurança da Informação	Versão: V4.0

6 GLOSSÁRIO

Não se aplica

7 ANEXOS

Não se aplica

8 QUADRO DE APROVAÇÃO

NOME	CARGO	ÁREA
Sandro Simas	Vice-presidente	Tecnologia

APROVADO PELO CONSELHO DE ADMINISTRAÇÃO DA V.TAL EM: 14/05/2025

ESTE DOCUMENTO REVOGA VERSÕES ANTERIORES