

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO



HISTÓRICO DE REVISÕES

REVISÃO	DATA	NATUREZA DA ALTERAÇÃO	APROVAÇÃO
00	02/10/2026	Emissão da versão para divulgação externa	Alta Direção

Sumário

1. INTRODUÇÃO	04
2. OBJETIVO	04
3. ABRANGÊNCIA	04
4. COMPROMISSO DA ALTA DIREÇÃO	04
5. PRINCÍPIOS	05
6. DIRETRIZES DE SEGURANÇA DA INFORMAÇÃO	06
7. PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS	09
8. OBJETIVOS, AVALIAÇÃO E MELHORIA	09
9. RESPONSABILIDADES	09
10. DOCUMENTOS COMPLEMENTARES	10
11. CANAIS DE CONTATO	10
12. REVISÃO E VIGÊNCIA	10

1. INTRODUÇÃO

A informação é um ativo essencial para as atividades da Velsis e para a confiança de clientes, colaboradores, parceiros, fornecedores e demais partes interessadas. Sua proteção contribui para a continuidade dos negócios, a qualidade dos produtos e serviços e o atendimento aos requisitos aplicáveis.

A Velsis mantém um Sistema de Gestão de Segurança da Informação certificado conforme a ISO/IEC 27001, dentro do escopo definido no certificado vigente.

2. OBJETIVO

Estabelecer os princípios e compromissos que orientam a proteção das informações sob responsabilidade da Velsis, preservando sua confidencialidade, integridade e disponibilidade e promovendo a gestão de riscos, a resiliência e a melhoria contínua.

3. ABRANGÊNCIA

Esta política aplica-se às atividades da Velsis e orienta administradores, colaboradores, prestadores de serviços, fornecedores, parceiros e demais partes que tratem informações ou utilizem recursos sob responsabilidade da organização. Requisitos específicos são definidos em contratos e documentos complementares aplicáveis.

4. COMPROMISSO DA ALTA DIREÇÃO

A Alta Direção apoia a governança da segurança da informação, promove sua integração aos processos de negócio, acompanha o desempenho do sistema de gestão e assegura recursos compatíveis com os riscos e as prioridades da organização.

5. PRINCÍPIOS



Confidencialidade: A informação deve ser acessada e divulgada somente por pessoas autorizadas e para finalidades legítimas.



Integridade: A informação deve ser protegida contra alteração, perda ou destruição indevida, preservando sua exatidão e confiabilidade.



Disponibilidade: A informação e os serviços relacionados devem estar disponíveis conforme as necessidades do negócio e os requisitos aplicáveis.



Gestão baseada em riscos: As decisões de segurança devem considerar o contexto, os riscos, os impactos e a proporcionalidade das medidas adotadas.



Responsabilidade compartilhada: A proteção da informação depende da atuação coordenada da liderança, das áreas de negócio, dos colaboradores e das partes externas envolvidas.



Melhoria contínua: O sistema de gestão e seus controles devem ser avaliados e aprimorados diante da evolução dos riscos, das operações, das tecnologias e dos requisitos aplicáveis.

6. DIRETRIZES DE SEGURANÇA DA INFORMAÇÃO

6.1

Governança, riscos e conformidade

A segurança da informação deve ser integrada à governança e à tomada de decisão. Os riscos e os requisitos legais, regulatórios, contratuais e internos devem ser identificados, avaliados, tratados e acompanhados conforme sua relevância.

6.2

Gestão de ativos e classificação da informação

As informações e os ativos associados devem possuir responsabilidades definidas e proteção compatível com sua criticidade, sensibilidade, valor e requisitos aplicáveis durante todo o ciclo de vida.

6.3

Identidades e controle de acesso

Os acessos físicos e lógicos devem ser autorizados, limitados ao necessário, revistos conforme os requisitos aplicáveis e protegidos por medidas proporcionais aos riscos. Responsabilidades conflitantes devem ser segregadas quando apropriado.

6.4

Pessoas, conscientização e uso aceitável

As pessoas com acesso a informações ou recursos devem conhecer suas responsabilidades, receber orientação compatível com suas atividades e utilizar os recursos de forma ética, legal e responsável.

6.5

Segurança física e tecnológica

Instalações, equipamentos, aplicações, serviços, redes e ambientes de processamento devem receber medidas de proteção compatíveis com sua criticidade e com os riscos identificados.

6.6

Proteção da informação

As informações devem ser protegidas durante o armazenamento, o processamento, a comunicação e a transferência. Controles criptográficos devem ser aplicados quando exigidos pela classificação da informação, pelos riscos ou pelos requisitos aplicáveis.

6.7

Segurança no ciclo de vida e gestão de mudanças

Requisitos de segurança devem ser considerados na aquisição, no desenvolvimento, na integração, na manutenção, na mudança e na descontinuação de produtos, serviços, soluções e processos.

6.8

Fornecedores e cadeia de suprimentos

Os relacionamentos com terceiros devem considerar riscos, responsabilidades, confidencialidade, continuidade, comunicação de incidentes e requisitos de segurança proporcionais ao serviço ou à informação envolvida.

6.9

Monitoramento e rastreabilidade

A Velsis mantém registros e atividades de monitoramento proporcionais aos riscos para apoiar a segurança, a continuidade, a conformidade e a proteção das informações.

6.10

Continuidade e resiliência

As medidas de continuidade devem ser planejadas, mantidas e avaliadas conforme os riscos e as prioridades do negócio, buscando preservar ou restabelecer atividades e serviços relevantes em situações adversas.

6.11

Gestão de incidentes

Eventos e suspeitas de segurança devem ser comunicados pelos canais institucionais aplicáveis. Os incidentes devem ser avaliados, tratados, registrados e utilizados como fonte de aprendizado, conforme sua natureza, seu impacto e as obrigações pertinentes.

6.12

Cenário de riscos e ameaças

A Velsis acompanha a evolução do cenário de riscos e ameaças para apoiar decisões e aprimorar continuamente suas medidas de proteção.

6.13

Comunicação responsável de vulnerabilidades

A Velsis incentiva clientes, parceiros e pesquisadores a comunicarem, de forma responsável e confidencial, possíveis vulnerabilidades identificadas em seus produtos, serviços ou ambientes, pelo canal indicado na seção 11. As comunicações recebidas são analisadas e tratadas conforme sua relevância.

7. PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS

A Velsis reconhece a privacidade e a proteção de dados pessoais como componentes da governança da informação. Os dados pessoais devem ser tratados de forma lícita, transparente e segura, para finalidades legítimas e com medidas proporcionais aos riscos, em conformidade com a Lei nº 13.709/2018 (LGPD).

As diretrizes específicas sobre coleta, uso, compartilhamento, retenção, direitos dos titulares e canais de atendimento estão disponíveis na Política de Privacidade da Velsis, acessível em: <https://velsis.com.br/governanca/>

8. OBJETIVOS, AVALIAÇÃO E MELHORIA

A Velsis estabelece objetivos de segurança da informação coerentes com sua estratégia e seus riscos. O desempenho do sistema de gestão é acompanhado e avaliado por meio de monitoramento, auditorias, análise crítica pela Alta Direção e outras verificações autorizadas.

Não conformidades, incidentes, mudanças e oportunidades de melhoria devem ser tratados de forma estruturada, com ações proporcionais e avaliação de eficácia.

9. RESPONSABILIDADES

A proteção da informação é uma responsabilidade compartilhada. A Alta Direção, os gestores, os colaboradores, os prestadores de serviços, os fornecedores e os parceiros devem observar as responsabilidades e os requisitos aplicáveis às suas atividades e aos relacionamentos mantidos com a Velsis.

O descumprimento desta política e de seus documentos complementares está sujeito às medidas previstas em normas internas, contratos e legislação aplicável.

10. DOCUMENTOS COMPLEMENTARES

Esta política é complementada por normas e procedimentos internos, cujo acesso e divulgação são definidos de acordo com seu conteúdo e classificação.

11. CANAIS DE CONTATO

Comunicações relacionadas a esta política devem ser encaminhadas pelos canais abaixo:

FINALIDADE	CANAL
Segurança da informação e comunicação de vulnerabilidades	seguranca@velsis.com.br
Privacidade e proteção de dados (Encarregado/DPO)	dpo@velsis.com.br

12. REVISÃO E VIGÊNCIA

Esta política entra em vigor na data indicada no controle do documento e deve ser revisada, no mínimo, anualmente ou diante de alterações relevantes no contexto, nos riscos, nas operações ou nos requisitos aplicáveis.



