

POLÍTICA

001 – Segurança da Informação

Revisão: 03 Ano: 2024 - Vigência: 17/01/2024

Próxima Revisão: 17/01/2026

CS - Cyber Security

Identificação: Política de Segurança da Informação			Nº 001
Prática: CS	Processo: Cyber Security	Data de Vigência: 17/01/2024	Data de Revisão: 17/01/2026

SUMÁRIO

1. OBJETIVO	3
2. ABRANGÊNCIA	3
3. REFERÊNCIAS	3
4. DEFINIÇÕES	3
5. DIRETRIZES GERAIS E ESPECÍFICAS	4
5.1. DIRETRIZES GERAIS.....	4
5.2. DIRETRIZES ESPECÍFICAS.....	4
6. MEDIDAS DISCIPLINARES	5
7. CONFIDENCIALIDADE	5
8. APROVAÇÕES	Erro! Indicador não definido.
9. HISTÓRICO DE REVISÕES	Erro! Indicador não definido.

Identificação: Política de Segurança da Informação			Nº 001
Prática: CS	Processo: Cyber Security	Data de Vigência: 17/01/2024	Data de Revisão: 17/01/2026

1. OBJETIVO

Garantir as diretrizes estratégicas de Segurança da Informação e, a partir da sua existência, normas corporativas e procedimentos operacionais, compondo assim um sistema normativo de Segurança da Informação, alinhada as boas práticas e normas internacionalmente aceitas, com o objetivo de garantir níveis adequados de proteção a informações da VEXIA ou sob sua responsabilidade.

Assegurar que os gestores possam realizar o gerenciamento da estrutura de Segurança da Informação da VEXIA, definindo, analisando e priorizando as ações necessárias para alcance dos objetivos estabelecidos pela VEXIA para a segurança das informações nos principais processos de negócio.

2. ABRANGÊNCIA

Aplica-se a todos os colaboradores, dentro ou fora das dependências da empresa, quando em cumprimento da jornada de trabalho. Inclui terceiros que se relacionam com a VEXIA, sejam eles fornecedores, representantes comerciais, prestadores de serviços, entre outros, representados tanto na figura de pessoa jurídica, quanto física.

3. REFERÊNCIAS

- ✓ ABNT NBR ISO/IEC 27001:2022 - "Segurança da Informação, Segurança Cibernética e Proteção à Privacidade – Sistemas de Gestão de segurança da informação - Requisitos";
- ✓ ABNT NBR ISO/IEC 27002:2022 - "Segurança da Informação, Segurança Cibernética e Proteção à Privacidade - Controles de segurança da informação";
- ✓ Legislação vigente.

4. DEFINIÇÕES

CONFIDENCIALIDADE: Garantia de que as informações sejam acessadas somente por aqueles expressamente autorizados e que sejam devidamente protegidas do conhecimento dos não autorizados.

DISPONIBILIDADE: Garantia de que as informações e os recursos de Tecnologia da Informação e Comunicação estejam disponíveis sempre que necessário e mediante a devida autorização para seu acesso ou uso.

INFORMAÇÃO: É o conjunto de dados que, processados ou não, podem ser utilizados para produção, transmissão e compartilhamento de conhecimento, contidos em qualquer meio, suporte ou formato.

INTEGRIDADE: Garantia de que as informações estejam fidedignas em relação à última alteração durante o seu ciclo de vida.

NORMAS COMPLEMENTARES: Trata-se das normas que complementam as diretrizes de uma política ou norma.

Identificação: Política de Segurança da Informação			Nº 001
Prática: CS	Processo: Cyber Security	Data de Vigência: 17/01/2024	Data de Revisão: 17/01/2026

SISTEMA NORMATIVO: É o conjunto formado por políticas e normas complementares.

TERCEIRO: Prestador de serviço, terceirizado, fornecedor, credenciado, consultor, instrutor e parceiro.

5. DIRETRIZES GERAIS E ESPECÍFICAS

5.1. DIRETRIZES GERAIS

Promover a confidencialidade, integridade e disponibilidade das informações, através do tratamento tempestivo de riscos de segurança da informação e conscientização das partes interessadas, buscando o armazenamento e compartilhamento seguro de dados alinhado aos requisitos contratuais e regulatórios vigentes.

A VEXIA adota todas as medidas necessárias para garantir que esta Política e suas Normas complementares sejam adequadamente comunicadas, entendidas e seguidas em todos os níveis da organização.

5.2. DIRETRIZES ESPECÍFICAS

- I. Toda informação gerada, armazenada, processada, administrada ou confiada à VEXIA é considerada de sua propriedade, estando regulamentada por esta Política de Segurança da Informação e suas Normas complementares, e sujeita à auditoria e monitoramento, visando garantir que a mesma seja utilizada por usuários devidamente autorizados, para fins profissionais, no estrito interesse da VEXIA;
- II. A informação gerada, armazenada, processada, administrada ou confiada à VEXIA deve ser classificada e tratada, quando possível, de modo adequado durante todo seu ciclo de vida, ou seja, manuseio, transmissão, transporte e descarte, seguindo níveis adequados de proteção, de acordo com seu grau de confidencialidade e relevância;
- III. Todos os profissionais, estagiários e prestadores de serviços devem receber o treinamento adequado quanto à manipulação da informação e ao uso dos recursos de tecnologia da informação, afim de garantir a proteção contra modificação não autorizada, uso indevido, destruição, desvio, acesso ou divulgação não autorizada, garantindo sua integridade, confidencialidade e disponibilidade;
- IV. As áreas de Segurança da Informação e Tecnologia de Infraestrutura e Comunicações devem monitorar e analisar o ambiente de tecnologia da VEXIA com o intuito de identificar e avaliar vulnerabilidades, riscos e impactos que possam causar indisponibilidades e incidentes;
- V. A segurança da informação deverá ser integrada, quando aplicável, no gerenciamento de projetos, visando assegurar que os riscos de segurança da informação serão identificados e avaliados como parte do projeto;
- VI. Uma avaliação dos riscos de segurança da informação deverá ser conduzida, quando aplicável, nos estágios iniciais dos projetos para identificar os controles necessários;

Identificação: Política de Segurança da Informação			Nº 001
Prática: CS	Processo: Cyber Security	Data de Vigência: 17/01/2024	Data de Revisão: 17/01/2026

- VII. Os processos críticos para o negócio da VEXIA devem fazer parte do Plano de Continuidade de Negócios, assegurando a sua recuperação e a continuidade dos processos em situações de contingência;
- VIII. Incidentes de segurança da informação devem ser tratados integralmente, garantindo que os mesmos sejam adequadamente registrados, classificados, investigados, corrigidos, documentados e, quando necessário, comunicado às autoridades apropriadas;
- IX. Todos os profissionais, parceiros, prestadores de serviços e estagiários que manipulem informações de propriedade da VEXIA devem assinar um Termo de Confidencialidade;
- X. A gestão de Segurança da Informação deve objetivar sempre a melhoria contínua através da definição e revisão sistemática de objetivos de segurança em todos os níveis da organização;
- XI. Requisitos de segurança da informação aplicáveis ou exigidos por regulamentações e/ou legislações vigentes devem ser atendidos de forma integral.

6. MEDIDAS DISCIPLINARES

O descumprimento das diretrizes estipuladas nesta Política caracteriza uma situação de não conformidade e para tanto, deverá ser apontada conforme procedimento específico, através da comunicação à área de *Compliance* ou à Linha Ética. Tal fato será objeto de avaliação e poderá levar à aplicação de medidas administrativas, conforme determina a Política de Medidas Disciplinares da VEXIA.

Aquele que adotar ações de retaliação contra qualquer pessoa que tenha, em boa-fé, suscitado questões ou preocupações de conformidade com esta política estará sujeito às mesmas sanções disciplinares.

7. CONFIDENCIALIDADE

Este documento é de propriedade da VEXIA, porém, em virtude de suas características, seu uso é **PÚBLICO**, podendo ser impresso, e/ou divulgado.