

DATA DE CRIAÇÃO	ÚLTIMA REVISÃO	CLASSIFICAÇÃO	APROVAÇÃO
Janeiro de 2024	Agosto de 2026	Uso Interno	Diretoria Executiva WFLOW

1. Introdução

A **WFLOW Consultoria** estabelece sua Política de Segurança da Informação e Cibernética em consonância com as exigências da Resolução CMN nº 4.893/2021 do Banco Central do Brasil, a Lei Geral de Proteção de Dados (LGPD nº 13.709/2018) e o Código ANBIMA de Regulação e Melhores Práticas [cite: 13]. Este normativo reflete o compromisso com a resiliência ciberestratégica e a salvaguarda de todos os ativos computacionais [cite: 13, 14].

2. Público-Alvo e Deveres Corporativos

A presente Política aplica-se integralmente a todas as **Pessoas Vinculadas** (sócios, diretores, colaboradores CLT, estagiários, prestadores de serviços, terceirizados e Agentes Autônomos de Investimento) [cite: 13].

Constituem obrigações imediatas de todas as Pessoas Vinculadas [cite: 13, 14]:

- Zelar por todo e qualquer acesso realizado e registrado sob sua identificação e credencial de rede [cite: 13];
- Preservar o sigilo e a confidencialidade das informações tratadas, vedada a divulgação não autorizada [cite: 13];
- Utilizar os recursos tecnológicos (hardware, software e e-mail) estritamente para finalidades profissionais [cite: 13];
- Abster-se de discutir ou compartilhar assuntos e dados confidenciais em locais públicos, redes sociais ou transportes [cite: 13];
- Reportar imediatamente ao departamento de TI ou Compliance qualquer suspeita ou ocorrência de incidente cibernético [cite: 14].

Infração Grave: A violação das regras de Segurança da Informação sujeitará o infrator a severas punições disciplinares, rescisão contratual e responsabilização legal por eventuais danos causados [cite: 14].

3. Objetivos Estratégicos

Assegurar a **Confidencialidade, Integridade e Disponibilidade (Triade CID)** dos dados e sistemas de informação da WFLOW, de seus veículos de investimento, clientes e parceiros [cite: 14]. O normativo estabelece requisitos de proteção para prevenir, detectar, responder e mitigar vulnerabilidades e ataques cibernéticos [cite: 14].

4. Pilares da Segurança da Informação

- **Confidencialidade:** Garantia de que a informação é acessível apenas a pessoas formalmente autorizadas, evitando vazamentos e exposições indevidas [cite: 14].
- **Integridade:** Salvaguarda da exatidão e completeza das informações e métodos de processamento, impedindo alterações não autorizadas [cite: 14].
- **Disponibilidade:** Garantia de que usuários autorizados tenham acesso oportuno e confiável aos dados e ativos sempre que necessário [cite: 14].

- **Acesso Controlado e Privilégio Mínimo:** Restrição de acesso aos sistemas baseada na estrita necessidade da função (Need-to-Know) [cite: 14, 15].

5. Matriz de Governança e Responsabilidades

Área / Instância	Responsabilidades em Segurança da Informação e Cibernética
Diretoria Executiva / Board	Aprovar a Política, assegurar recursos para a infraestrutura de segurança e responder pela continuidade do negócio [cite: 15].
Tecnologia da Informação (TI)	Gerenciar o ambiente tecnológico, implantar Firewalls, Antivírus/E-DR, backups, gestão de acessos, testes de intrusão e resposta a incidentes [cite: 15].
Compliance e Risco	Acompanhar atualizações regulatórias, monitorar riscos cibernéticos, coordenar o DPO e atuar na gestão de não conformidades [cite: 15].
Jurídico	Garantir cláusulas rígidas de cibersegurança, confidencialidade e LGPD em contratos com terceiros e fornecedores [cite: 16].
Auditoria Interna	Avaliar periodicamente a eficácia dos controles lógicos, físicos e procedimentos de segurança da informação [cite: 16].

6. Mapeamento e Gestão de Riscos Cibernéticos

Conforme o Guia ANBIMA de Cibersegurança, a WFLOW mantém monitoramento contínuo sobre as principais ameaças [cite: 16]:

- Ataques por *Malwares*, *Ransomware* e técnicas sofisticadas de Engenharia Social (Phishing) [cite: 16];
- Vazamento, revelação ou modificação não autorizada de informações sensíveis [cite: 16];
- Ataques de negação de serviço (DDoS) e intromissão em redes corporativas [cite: 16];
- Interrupção de serviços operacionais críticos e danos reputacionais decorrentes de incidentes [cite: 16].

7. O Processo Quinquenário de Segurança Cibernética (ANBIMA)

A estrutura de proteção da WFLOW desenvolve-se através de 5 funções integradas [cite: 17]:

Função	Controles Operacionais e Ferramentas Aplicadas
1. Identificação / Avaliação	Mapeamento e inventário de ativos de informação e execução permanente de análise de vulnerabilidades [cite: 17].
2. Prevenção e Proteção	Controle de acesso lógico com duplo fator (MFA), senhas complexas, filtro web (Firewall), encriptação de discos e controle de privilégios de administrador [cite: 17, 18].
3. Monitoramento e Testes	Sensores de intrusão, simulações periódicas de phishing com colaboradores e testes de penetração (PenTest) externos [cite: 18].
4. Plano de Resposta a Incidentes	Alertas automatizados de paralisação, isolamento de máquinas infectadas e comunicação imediata à Diretoria e órgãos reguladores [cite: 18].
5. Governança e Comitê	Comitê de Segurança da Informação para reporte executivo, revisão do Plano de Continuidade e notificação à ANPD em caso de incidentes [cite: 18].

8. Acesso Remoto Seguro (VPN)

Conexão Criptografada: O trabalho remoto exige o uso obrigatório de Rede Virtual Privada (VPN) com criptografia forte e autenticação por múltiplos fatores (MFA) [cite: 18, 19]. É vedada a utilização de redes Wi-Fi públicas sem proteção [cite: 18].

9. Requisitos para Fornecedores e Partes Externas

A contratação de fornecedores de TI e processamento de dados exige homologação rigorosa [cite: 19]. Os contratos obrigatoriamente contemplam obrigações de criptografia, segmentação de rede, plano de resposta a incidentes e submissão às normas da Resolução CMN nº 4.893/2021 [cite: 19].

10. Descarte Seguro de Informações e Treinamento

A eliminação de mídias e documentos digitais é feita de maneira irreversível ao término do prazo de guarda regulatório [cite: 19, 20]. A WFLOW realiza treinamentos contínuos obrigatoriamente a todas as Pessoas Vinculadas para reciclar conceitos de proteção de dados, engenharia social e higiene cibernética [cite: 20].

11. Termo de Responsabilidade e Ciência

A adesão a este normativo é formalizada mediante a assinatura do **Termo de Responsabilidade e Ciência dos Normativos Corporativos** por ocasião da integração do profissional à WFLOW Consultoria [cite: 20].