Política de Segurança Cibernética

Neves Asset Management Ltda.

2025

1. Introdução

A Neves Asset Management Ltda. ("Neves Asset") reconhece que a informação é um ativo estratégico essencial para a continuidade, a reputação e a conformidade da organização. A presente Política de Segurança Cibernética tem como finalidade estabelecer as diretrizes que asseguram a proteção dos dados e sistemas da empresa contra ameaças internas e externas, acidentais ou deliberadas, promovendo a integridade, a confidencialidade, a autenticidade, a disponibilidade e a rastreabilidade das informações.

Esta política está alinhada com as exigências da Resolução CMN nº 4.893/2021, da Resolução BCB nº 85/2021, da Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e com as melhores práticas nacionais e internacionais aplicáveis à segurança cibernética no setor financeiro.

2. Abrangência

Esta política se aplica a todos os sócios, administradores, colaboradores, estagiários, prestadores de serviço, fornecedores e quaisquer terceiros que, de forma direta ou indireta, tenham acesso a dados, sistemas, redes, equipamentos ou qualquer recurso tecnológico da Neves Asset. A adesão às diretrizes aqui estabelecidas é condição obrigatória para a atuação dessas partes no âmbito da empresa.

3. Princípios Gerais

A segurança cibernética na Neves Asset pauta-se pelos seguintes princípios: (i) confidencialidade, assegurando que apenas pessoas autorizadas tenham acesso às informações; (ii) integridade, garantindo que os dados não sejam alterados de forma indevida; (iii) disponibilidade, permitindo que os sistemas e informações estejam acessíveis sempre que necessário; (iv) autenticidade, assegurando a veracidade da origem dos dados; e (v) conformidade, garantindo aderência às normas internas, legais e regulatórias aplicáveis.

4. Gestão de Acessos e Identidades

Os acessos a sistemas, redes e informações da Neves Asset serão concedidos conforme o princípio do menor privilégio, com base na função e na real necessidade do usuário. O controle de acesso será realizado por meio de identificadores individuais e intransferíveis, sendo obrigatória a utilização de senhas fortes e, sempre que possível, autenticação multifator. O desligamento de qualquer colaborador ou prestador de serviço implicará no imediato bloqueio de seus acessos.

5. Segurança da Infraestrutura e dos Ativos

Todos os ativos de informação deverão ser inventariados e classificados segundo seu grau de sensibilidade. Equipamentos e sistemas estarão protegidos contra o uso não autorizado, devendo as configurações de segurança atenderem aos padrões definidos pela área de tecnologia da Neves Asset. O uso de dispositivos pessoais em redes corporativas é restrito e sujeito a autorização e monitoramento.

A empresa manterá soluções atualizadas de proteção contra códigos maliciosos, antivírus, firewall e sistemas de detecção de intrusão. Todos os softwares utilizados deverão ser homologados e legalmente licenciados. A realização de cópias de segurança (backups) será conduzida com frequência definida e armazenada de forma segura, permitindo a recuperação adequada das informações.

6. Gestão de Risco e Vulnerabilidades

A Neves Asset manterá processo contínuo de identificação, análise, tratamento e monitoramento de riscos cibernéticos. Vulnerabilidades deverão ser tratadas com prioridade de acordo com seu potencial impacto, sendo as correções aplicadas em prazos compatíveis com a criticidade do risco. A empresa realizará periodicamente testes de segurança e simulações de ataque (testes de penetração), com o objetivo de avaliar a robustez dos controles implementados.

7. Prevenção e Resposta a Incidentes

A empresa disporá de procedimentos formais para resposta a incidentes de segurança da informação e cibernética, contemplando a identificação, comunicação, contenção, análise, erradicação e recuperação de eventuais falhas ou ataques. Incidentes relevantes serão reportados à alta administração, aos órgãos reguladores e, quando aplicável, aos titulares dos dados afetados. As ações de resposta serão documentadas e analisadas para identificação de causas e prevenção de recorrência.

8. Terceiros e Fornecedores

Todos os fornecedores e prestadores de serviços com acesso a informações ou sistemas da Neves Asset deverão aderir às exigências de segurança da informação e segurança cibernética estabelecidas em contrato. Será exigido que tais terceiros comprovem possuir controles compatíveis com os padrões da empresa, incluindo cláusulas sobre confidencialidade, proteção de dados e resposta a incidentes.

9. Monitoramento e Auditoria

As atividades e acessos a sistemas e informações serão monitorados de forma contínua, com logs armazenados em

ambiente seguro e protegidos contra alterações. Auditorias internas e externas poderão ser realizadas com o objetivo de verificar a aderência às diretrizes desta política e recomendar melhorias.

10. Disposições Finais

O descumprimento das disposições desta política está sujeito às medidas disciplinares previstas nas normas internas da empresa e na legislação aplicável. Esta política será revista anualmente ou sempre que houver mudanças relevantes no ambiente tecnológico, organizacional ou regulatório. Sua versão atual foi aprovada pelo Diretor de Compliance/PLD/Risco da Neves Asset Management Ltda.

Versão	Data da Atualização
1.1	Junho 2026