RESUMO

Política de Segurança Cibernética

Empresa: Nagro SCD S.A. — Sociedade de Crédito Direto
Versão: 1.0 | Vigência: junho/2026 a junho/2027
Classificação: Documento público — resumo para divulgação no site institucional
Referências regulatórias: Resolução CMN nº 5.274/2025 | Resolução BCB nº 538/2025

Sobre esta política

A Nagro SCD mantém uma Política de Segurança Cibernética formal, aprovada pela Diretoria Executiva, em conformidade com a Resolução CMN nº 5.274/2025, a Resolução BCB nº 538/2025 e demais normativos do Conselho Monetário Nacional e do Banco Central do Brasil. Este documento estabelece os princípios, diretrizes, responsabilidades e controles mínimos que protegem a confidencialidade, integridade, disponibilidade e autenticidade das informações e sistemas da Instituição — e, por consequência, os dados de nossos clientes, parceiros e colaboradores.

A Política abrange todos os sistemas, plataformas, ambientes (produção, homologação, desenvolvimento e testes) e ativos físicos e lógicos sob gestão da Nagro SCD, bem como os serviços prestados por terceiros que integram nossa cadeia de valor, incluindo provedores de computação em nuvem, processadores de pagamento e desenvolvedores de software. É de observância obrigatória por colaboradores, administradores, estagiários, prestadores de serviço e demais terceiros com acesso, ainda que temporário, aos nossos ativos de informação.

Princípios que orientam nossa atuação

Nossa gestão de segurança cibernética é fundamentada nos seguintes princípios:

- Confidencialidade — as informações são acessíveis somente por pessoas autorizadas;
- Integridade — as informações são precisas, completas e protegidas contra alterações não autorizadas;
- Disponibilidade — sistemas e informações estão acessíveis quando necessários para suportar nossas operações;
- Autenticidade — a identidade dos usuários e a origem das informações são verificáveis;
- Não-repúdio — as ações realizadas sobre ativos de informação são rastreáveis e atribuíveis ao responsável;
- Proporcionalidade — os controles são proporcionais ao risco, criticidade e sensibilidade dos ativos protegidos;
- Resiliência — mantemos capacidade de absorver, adaptar-nos e recuperar-nos de incidentes cibernéticos;
- Melhoria contínua — controles e processos de segurança são revisados e aprimorados de forma sistemática e periódica.

Governança de segurança cibernética

A segurança cibernética é tratada como responsabilidade compartilhada, com papéis claramente definidos em três níveis:

Diretoria Executiva

Aprova a Política e suas revisões periódicas, garante a alocação de recursos humanos, tecnológicos e financeiros adequados, define o apetite de risco cibernético da Instituição e é informada sobre incidentes de alta severidade e sobre o desempenho do programa de segurança cibernética ao menos semestralmente.

Área de GRC & Segurança da Informação (CISO)

Implementa, mantém e revisa esta Política e os documentos normativos correlatos; gerencia o programa de segurança cibernética — riscos, controles, incidentes e conformidade regulatória; conduz ou supervisiona avaliações de risco, testes de intrusão e auditorias de segurança; reporta à Diretoria Executiva sobre o estado da segurança cibernética; e atua como ponto focal junto ao Banco Central do Brasil para comunicações relacionadas a segurança e a incidentes relevantes.

Colaboradores e usuários

Todos os colaboradores, prestadores de serviço e terceiros são responsáveis por conhecer e cumprir esta Política, utilizar os ativos de informação exclusivamente para fins relacionados às atividades da Instituição, não compartilhar credenciais de acesso, participar dos treinamentos de conscientização e reportar imediatamente qualquer suspeita de incidente de segurança aos canais designados (vide seção “Canais de Contato” ao final deste resumo).

Gestão de riscos cibernéticos

Adotamos processo formal e contínuo de gestão de riscos, estruturado em cinco etapas: identificação e inventário de ativos, ameaças e vulnerabilidades; análise e avaliação de probabilidade e impacto; tratamento (mitigar, aceitar, transferir ou evitar); monitoramento e revisão contínua da eficácia dos controles; e comunicação às partes interessadas, incluindo o regulador quando aplicável. A avaliação de riscos é realizada ao menos anualmente, ou sempre que ocorrerem mudanças significativas em sistemas, processos, infraestrutura ou no ambiente regulatório.

Os resultados subsidiam o Plano de Ação em Segurança Cibernética (PASC), documento formal revisado anualmente que reúne as ações priorizadas de tratamento de riscos, cronograma de implementação de controles, critérios de aceitação de riscos residuais e indicadores de acompanhamento (KPIs e KRIs).

Controle de acesso e identidade

- Princípio do menor privilégio — cada usuário recebe apenas as permissões estritamente necessárias ao exercício de suas funções, com segregação de funções para evitar concentração de poder em etapas críticas;
- Autenticação multifator (MFA) obrigatória — exigida para acesso remoto, consoles e CLI em nuvem, contas privilegiadas e todos os sistemas com dados financeiros ou pessoais de clientes; métodos aceitos incluem aplicativos autenticadores

(TOTP), chaves de segurança físicas (FIDO2/WebAuthn) e push notification — o uso de SMS é vedado para sistemas críticos e contas privilegiadas;

- Gestão do ciclo de vida de acessos — concessão formal, revisão semestral e revogação imediata em casos de desligamento ou mudança de função;
- Política de senhas e contas privilegiadas — troca imediata em caso de suspeita de comprometimento, intervalo máximo de 180 dias para contas privilegiadas, que são nominais, auditadas e monitoradas continuamente;
- Acesso de terceiros — fornecedores estão sujeitos aos mesmos requisitos de MFA, como condição contratual obrigatória.

Proteção de dados e criptografia

- Criptografia em trânsito — toda comunicação de dados sensíveis utiliza protocolos seguros (TLS 1.2 ou superior, SSH, SFTP), sendo vedados protocolos inseguros;
- Criptografia em repouso — dados pessoais, financeiros, credenciais e informações confidenciais são armazenados com criptografia robusta (AES-256 ou equivalente), incluindo proteção adicional em nível de campo para CPF, dados bancários e informações de crédito;
- Gestão de chaves e certificados — chaves criptográficas são gerenciadas por sistema dedicado, com rotação periódica, princípio do menor privilégio e separação entre ambientes; certificados digitais seguem processo formal de emissão, renovação antecipada e monitoramento contínuo, sendo vedados certificados autoassinados em produção;
- Descarte seguro — ativos, mídias físicas e volumes de armazenamento que contenham dados confidenciais passam por sanitização ao final do ciclo de vida, impedindo a recuperação das informações por terceiros.

Segurança em nuvem e infraestrutura

Nosso ambiente tecnológico é majoritariamente baseado em nuvem, operado por provedores de grande porte e referência mundial. Mantemos modelo de responsabilidade compartilhada documentado com os provedores, configurações seguras (hardening) baseadas em padrões reconhecidos internacionalmente (CIS Benchmarks), segmentação entre ambientes de produção, homologação e desenvolvimento, detecção automática de desvios de configuração e revisão trimestral de permissões e configurações. O uso de softwares e sistemas em fim de vida (EOL/EOS) é vedado em produção, e nossos pipelines de integração e entrega contínua (CI/CD) possuem controles de acesso restritos, gestão de segredos e auditoria de alterações.

Monitoramento, logs e rastreabilidade

Mantemos capacidade estruturada de monitoramento e rastreabilidade das atividades em nossos sistemas, com coleta centralizada de eventos, registros que incluem identificação do solicitante, origem e resultado das operações, e trilhas de auditoria específicas para operações financeiras (desembolso, cessão, boletagem e renegociação). Dados sensíveis — como CPF, dados bancários, tokens, e-mail e telefone — são mascarados antes da ingestão nos sistemas de coleta. Os logs são mantidos por, no mínimo, 5 (cinco) anos, de forma imutável e protegida contra exclusão não autorizada, conforme a Res. CMN 5.274/2025.

Operamos plataforma de SIEM (Security Information and Event Management) como motor central de correlação de eventos e detecção de incidentes, recebendo dados de sistemas em nuvem, endpoints (EDR), APIs e provedores de identidade, com alertas automáticos para falhas de autenticação, acessos fora do horário comercial, volumes anômalos de exportação de dados e demais cenários de risco. Os registros de fornecedores e integrações externas também integram esse escopo de rastreabilidade.

Gestão de vulnerabilidades e testes de segurança

- Varreduras automatizadas de vulnerabilidades em toda a infraestrutura, com periodicidade ao menos mensal;
- Gerenciamento de patches com prazos definidos por criticidade: até 72 horas para vulnerabilidades críticas, 7 dias para altas, 30 dias para médias e prazos específicos para baixas e informativas;
- Testes de intrusão (pentests) por empresa independente ao menos uma vez ao ano, cobrindo sistemas críticos, APIs e infraestrutura em nuvem, com retest obrigatório para achados críticos ou altos e relatório dedicado para fins regulatórios;
- Práticas de DevSecOps — análise estática (SAST), dinâmica (DAST) e revisão de segurança antes da publicação em produção, com varredura de imagens de contêiner antes de cada implantação;
- Quando não há correção disponível (zero-days, sistemas legados), aplicamos controles compensatórios — isolamento, regras de bloqueio, restrição de acesso e abertura formal de Risco Aceito, com aprovação do CISO e reavaliação periódica.

Inteligência de ameaças (Threat Intelligence)

Participamos de fontes de inteligência relevantes ao setor financeiro (como CERT.br e CISA), contamos com fornecedor especializado em Cyber Threat Intelligence para monitoramento de fontes externas (deep web, fóruns e exposição de marca), acompanhamos ameaças emergentes voltadas a fintechs e sistemas de crédito, integramos indicadores de comprometimento aos nossos controles de detecção e participamos de mecanismos de compartilhamento de informações sobre incidentes e ameaças com outras

instituições autorizadas pelo Banco Central, fortalecendo a resiliência do Sistema Financeiro Nacional.

Gestão de incidentes cibernéticos

Mantemos Plano de Resposta a Incidentes (PRI) formal, atualizado e testado por meio de simulações (tabletop exercises) ao menos semestralmente — incluindo cenários de alta complexidade, como sequestro de dados (ransomware), interrupção de serviços em nuvem e comprometimento da cadeia de suprimentos de software. O plano disciplina a identificação e classificação por severidade, contenção, erradicação, recuperação, análise pós-incidente e a comunicação tempestiva ao Banco Central do Brasil — em até 4 horas para incidentes críticos —, nos termos da Res. CMN 5.274/2025 e da Res. BCB 538/2025.

O PRI e o Plano de Continuidade de Negócios (PCN) são interdependentes e acionados de forma integrada sempre que a severidade de um incidente ameaçar a continuidade das operações críticas, com decisão conjunta entre o CISO e a Diretoria Executiva.

Continuidade de negócios e recuperação de desastres

Mantemos Plano de Continuidade de Negócios (PCN) e Plano de Recuperação de Desastres (PRD), com Objetivos de Tempo de Recuperação (RTO) e de Ponto de Recuperação (RPO) definidos para cada sistema e processo crítico — revisados anualmente. Realizamos backups regulares com testes periódicos de restauração, replicação em local segregado com proteção criptográfica e, sempre que possível, cópias em formatos imutáveis ou protegidos contra deleção maliciosa. Testes de continuidade e recuperação são realizados ao menos anualmente, e um Plano de Comunicação de Crise define canais, responsáveis e prazos para informar clientes, reguladores e parceiros em cada nível de severidade, incluindo as obrigações de notificação ao Banco Central e aos titulares de dados pessoais nos termos da LGPD.

Segurança na gestão de terceiros e fornecedores críticos

- Due diligence de segurança cibernética antes da contratação, incluindo avaliação de controles e certificações como ISO 27001, SOC 2, LGPD e PLD/FT;
- Cláusulas contratuais específicas de segurança, confidencialidade, direito de auditoria e obrigações em caso de incidente, com notificação imediata por parte do fornecedor;
- Classificação de fornecedores por criticidade, com controles proporcionais ao risco e monitoramento contínuo de desempenho e conformidade;

- Avaliação periódica do risco de concentração em fornecedores e dos planos de continuidade dos próprios terceiros, garantindo alinhamento de RTO/RPO;
- Monitoramento contínuo do risco cibernético em fornecedores por meio de ferramenta de Supply Chain Security Intelligence, com scoring de maturidade e alertas de comprometimento.

Segurança física, endpoints e proteção contra código malicioso

- Solução de Endpoint Detection and Response (EDR) e proteção para workloads em nuvem (CWPP) em todos os dispositivos e ambientes gerenciados, com integração ao SIEM;
- Criptografia de disco completo em laptops e dispositivos móveis, e controle de privilégios para estações e dispositivos;
- Gateway de segurança de e-mail com varredura de anexos, sandboxing, filtragem de URLs maliciosas e configurações DMARC, DKIM e SPF;
- Filtragem de DNS/URLs, restrição de execução de macros e scripts, e bloqueio ou varredura obrigatória de mídias removíveis (USB);
- Controle de acesso físico às instalações por catraca biométrica, biometria e segurança armada — observando que nosso ambiente tecnológico é majoritariamente em nuvem, sem servidores locais sob gestão direta da Nagro SCD.

Desenvolvimento seguro e segurança de APIs

Adotamos práticas de Secure Software Development Lifecycle (SSDLC), com requisitos de segurança desde a fase de design, revisões de código focadas em segurança para funcionalidades críticas, ferramentas de análise estática (SAST) e dinâmica (DAST) integradas ao pipeline de CI/CD, e proteção de APIs com autenticação robusta (OAuth 2.0), limitação de taxa de requisições (rate limiting), validação de entrada e monitoramento de uso anômalo. O uso de segredos — chaves, senhas ou tokens — diretamente em código-fonte ou repositórios é expressamente proibido.

Treinamento, conscientização e indicadores

Promovemos treinamentos e ações contínuas de conscientização sobre segurança cibernética para colaboradores, prestadores de serviço e parceiros, fortalecendo uma cultura organizacional de proteção de dados e sistemas. O desempenho do programa de segurança cibernética é acompanhado por indicadores-chave (KPIs e KRIs) e reportado periodicamente à Diretoria Executiva, subsidiando o ciclo contínuo de melhoria dos controles.

Canais de contato — Segurança da Informação

Asseguramos a colaboradores, clientes, prestadores de serviço e terceiros o direito de reportar, de boa-fé e sem qualquer forma de retaliação, discriminação ou prejuízo funcional, suspeitas de incidentes de segurança, violações desta Política ou comportamentos que possam representar risco aos nossos ativos de informação. Os canais disponíveis são:

- E-mail de Segurança da Informação — seginfo@nagro.com.br, canal monitorado pela área de GRC & Segurança da Informação, para reporte de incidentes, suspeitas e dúvidas relacionadas à segurança cibernética;
- Canal de denúncia anônima — disponível conforme a política interna de compliance e ética da Nagro SCD, para reportes que o denunciante prefira realizar sem identificação;
- Equipe de Segurança da Informação — suspeitas de incidentes também podem ser reportadas diretamente ao time de segurança da informação, com prioridade máxima de comunicação.

Recomendamos que qualquer suspeita seja comunicada com a maior brevidade possível, de modo a permitir resposta ágil e reduzir eventuais impactos.

Vigência e revisão

Esta política foi aprovada pela Diretoria Executiva da Nagro SCD, possui vigência de junho/2026 a junho/2027, e é revisada anualmente ou sempre que ocorrerem mudanças relevantes em nossos sistemas, processos ou no ambiente regulatório. Este resumo público reflete o conteúdo vigente da Política de Segurança Cibernética da Nagro SCD S.A. e é disponibilizado para fins de transparência institucional.