N26

Política de Segurança Cibernética

n26brasil.com

Edição Dez 2022
N26 SOCIEDADE DE CRÉDITO DIRETO S.A.

Política de Segurança Cibernética

1.1. Introdução

A N26 Sociedade de Crédito Direto S.A. (“N26 SCD” ou “Instituição”) é uma sociedade de crédito direto autorizada a funcionar pelo Banco Central do Brasil, com objetivo de oferecer uma conta digital aos clientes com propósito de auxiliar na educação financeira, dentre outros.

Esta Política se aplica aos diretores, a todos os colaboradores e a todos os terceiros externos como clientes, parceiros, agentes públicos e fornecedores da N26 SCD.

1.2. Objetivo

Esta Política visa garantir o cumprimento das exigências regulatórias previstas pela Resolução 4.893/21 do Conselho Monetário Nacional e objetiva estabelecer os princípios, diretrizes e atribuições relacionadas à segurança cibernética, respeitando o porte, o perfil de risco e o modelo de negócio da N26 SCD.

1.3. Os princípios da segurança cibernética

A segurança cibernética possui princípios que visam conscientizar e prover proteção dos ativos e informações da empresa, também gerando prevenção para o entendimento de futuros incidentes ou problemas de segurança cibernética. Nesta política, vamos abordar a segurança cibernética sob a ótica dos seguintes princípios:

- ➔ Confidencialidade: garantia que a informação estará acessível apenas para pessoas autorizadas.
- ➔ Integridade: manutenção das condições iniciais das informações de acordo com a forma que foram produzidas e armazenadas.
- ➔ Disponibilidade: os dados corporativos precisam estar seguros e disponíveis para serem acessados a qualquer momento pelos usuários autorizados.

Para a N26 SCD garantir confidencialidade, integridade e disponibilidade é fundamental para a segurança e consistência de nossos dados e sistemas,

por meio do mapeamento do ambiente digital de sua atuação, bem como suas interações com este ambiente.

1.4. Das responsabilidades dos departamentos da N26 SCD para segurança cibernética

Os departamentos da N26 SCD têm o dever de respeitar o disposto nesta política, buscando-a para sanar potenciais dúvidas e caso não sendo possível, procurar o time de segurança da informação para dirimir qualquer questão.

É de responsabilidade da do time de Segurança da Informação criar procedimentos adequados visando diminuir a vulnerabilidade e potenciais incidentes e divulgá-los utilizando os canais e meios corretos. As responsabilidades específicas de cada departamento serão tratados em documentos específicos contendo os procedimentos detalhados para os casos tratados.

1.5. Dos procedimentos e controles da N26 SCD para segurança cibernética

É dever da N26 SCD possuir todo o registro de atividades de maneira a realizar a rastreabilidade das informações com o propósito de garantir o tratamento correto das informações tidas como sensíveis nos manuais e procedimentos da companhia.

O procedimento em relação aos efeitos dos incidentes será tratado pelo time de segurança cibernética, mantendo sempre o registro do incidente, a análise do problema, qual foi a resolução e criando relatório ao final e submetendo a análise e assinatura digital do diretor da área. Todos os potenciais incidentes de segurança têm seus cenários considerados nos testes de continuidade de negócios para todos os sistemas integrantes da N26 SCD.

Os procedimentos e controles descritos serão realizados com frequência mínima anual e todos com camadas de proteção abrangendo: autenticação, criptografia, prevenção e detecção de intrusão, prevenção de vazamento de informações, realização periódica de testes e varreduras para detecção de vulnerabilidades, proteção contra softwares maliciosos, estabelecimento de mecanismos de rastreabilidade, controles de acesso e segmentação da rede de computadores e manutenção de cópias de segurança de dados e informações.

1.5.1 Acesso a sistemas, recursos e ativos de informação:

Os acessos a sistemas, recursos e ativos de informação dentro da N26 Brasil devem ser concedidos mediantes uma autenticação e solicitação válida e baseada em:

- ➔ Necessidade de negócio
- ➔ O princípio de menor privilégio; e
- ➔ Segregação de funções

Sempre que um funcionário precisa de acesso a um dado PII (dado sensível), por exemplo, o mesmo deve submeter uma solicitação através da Central de Ajuda, justificando a necessidade do seu acesso àquela informação. Os privacy champions são responsáveis por aprovar essa solicitação e então conceder acesso àquela informação.

Os acessos aos sistemas e recursos da N26 Brasil se dão através de tecnologias de login único, sendo assim, todos os acessos são segregados em grupos, por áreas, e as permissões de cada funcionário são concedidas apenas para que realizem o necessário, seguindo o princípio de menor privilégio.

Todos os acessos são gerenciados através de um ciclo de vida, desde o momento da criação até a desativação (para desligamentos de colaboradores) incluindo revisões periódicas quanto a precisão.

1.5.2 Rastreabilidade:

As ações executadas em ambientes tecnológicos da N26 Brasil são capazes de rastreio, registrando:

- ➔ A atividade foi executada
- ➔ Quem executou a atividade
- ➔ Quando a atividade foi executada

Histórico e trilhas de auditoria são habilitadas em todos os ambientes produtivos, protegidos de acessos e alterações indevidas.

1.5.3 Prevenção, detecção e identificação de ataques:

A infraestrutura tecnológica da N26 Brasil é monitorada a fim de garantir a segurança dos recursos e ativos de informação em nosso ambiente em

nuvem. Sistemas de detecção e prevenção de invasões são implementados com um processo de resposta definido.

A infraestrutura em nuvem da N26 Brasil, conta com:

- ➔ Sistema de detecção de invasões em nuvem
- ➔ Sistema de prevenção de invasões em nuvem
- ➔ SOC, Security Operations Center 24x7

O time de segurança da informação da N26 Brasil recebe alertas das ferramentas de monitoramento e da empresa que faz o papel de SOC e atua em cima de cada caso de forma imediata.

1.5.4 Plano de resposta a incidentes e tratamento:

Os planos de resposta de incidentes serão realizados seguindo os procedimentos definidos internamente pela equipe de Segurança Cibernética e oficializados em manual para tratar do tema e mantido em sistema de acesso de documentos.

Todo plano de resposta de incidente contém:

- ➔ ações de adequação da estrutura organizacional e operacional ligadas aos princípios N26 SCD;
- ➔ as rotinas com os procedimentos e os controles a serem realizados na utilização na prevenção de resposta a incidentes seguindo o disposto nesta política;
- ➔ todas as áreas responsáveis e envolvidas pelo tratamento, registro e controle dos efeitos dos incidentes mais relevantes da companhia;
- ➔ cenários padrões de incidentes de segurança e suas respectivas respostas padrões;

O processo de resposta e gestão de incidentes serão tratados apartado desta política, seguindo os procedimentos descritos e devidamente documentados na plataforma de gestão de documentos utilizada pela N26 SCD.

O processo segue os passos descritos abaixo:

- ➔ Problema é reportado por qualquer colaborador da N26 SCD em canal apropriado;
- ➔ Um profissional realiza a triagem do problema;
  - ◆ O Caso a triagem conclua que é incidente, é aberto no canal de incidentes um chamado para tratativa;
  - ◆ O Caso a triagem conclua que não é incidente, o problema é tratado pelo time responsável, com a devida priorização.
- ➔ A tarefa classificada como "Incidente" é criada na plataforma de gestão de projetos;

- ➔ O time de resposta ao incidente é recrutado pelo colaborador que reportou o incidente que será o ponto focal para a tratativa;
- ➔ É realizado diagnóstico do incidente;
- ➔ Ocorre a validação das tratativas e solução do incidente;
- ➔ O incidente segue monitorado;
- ➔ Realiza-se o procedimento de Post-mortem do incidente;

Dentro da N26 Brasil, classificamos os incidentes em 4 categorias de severidade:

- ➔ Crítico
- ➔ Alto
- ➔ Médio
- ➔ Baixo

1.5.5 Proteção a vazamento de dados:

Os ativos de informação da N26 Brasil devem estar protegidos e acessados apenas por pessoas autorizadas. Toda informação sensível deve ser acessada apenas mediante autorização prévia e baseada na necessidade justificada do acesso.

As informações são protegidas e monitoradas por ferramentas integradas aos nossos sistemas de armazenamento de dados, e possuímos:

- ➔ Sistema de DLP (Data Loss Prevention) integrado às ferramentas de trabalho, como por exemplo: correio eletrônico, salas virtuais e armazenamento em nuvem de dados, planilhas e documentos.
- ➔ Recursos restritos apenas a rede interna, acessada apenas através VPN.

1.5.6 Proteção a softwares maliciosos:

Todo o parque tecnológico da N26 Brasil é monitorado e controlado remotamente para garantir a segurança dos colaboradores e dos nossos recursos e ativos de informação. Os meios de armazenamento considerados como mídias removíveis possuem acesso controlado e quando não utilizados são protegidos utilizando criptografia.

Todas as máquinas passam por atualizações de sistemas remotamente, e são monitoradas através de um serviço de proteção local. Dessa forma, é possível garantir que:

- ➔ Todas as máquinas estão sempre com as últimas atualizações de segurança.

- ➔ Os colaboradores não conseguem acessar sites maliciosos e indevidos que possam comprometer algum ativo de informação armazenado localmente em sua estação de trabalho.
- ➔ Todas as máquinas contam com políticas de senhas, proteção de dispositivos móveis e criptografia de disco.
- ➔ Acesso remoto às estações de trabalho em casos de resposta a incidentes.

1.5.7 Relatório anual de cyber:

Todos os incidentes que acontecem na N26 Brasil são controlados e seguem um padrão de escrita para os Reportes de Incidentes.

O relatório anual com data base de 31 de dezembro do ano anterior, contendo os reportes de incidentes será elaborado e aprovado até o dia 31 de março do ano corrente pelo Comitê de Compliance, Riscos e Prevenção à Lavagem de Dinheiro e Financiamento ao Terrorismo.

1.5.8 Gerenciamento de vulnerabilidades

O gerenciamento de vulnerabilidades se dá através de um ciclo de vida, desde a identificação até a remediação.

Todas as alterações realizadas em nossos produtos, passam por uma análise automatizada de regras de segurança para garantir que o que desenvolvemos é seguro. As vulnerabilidades identificadas são reportadas para os respectivos times e os mesmos encarregam-se de mitigá-las com o auxílio do time de Segurança. Quando uma vulnerabilidade não pode ser corrigida imediatamente, o time de Segurança avalia a possibilidade de aceitar este risco.

É proibido aceitar vulnerabilidades de criticidade alta, portanto, quando as mesmas surgem, devem ser corrigidas.

Varreduras automatizadas são realizadas bimestralmente em nossas principais aplicações, por uma consultoria externa, a fim de identificar falhas de segurança do ponto de vista externo. Todas as vulnerabilidades encontradas são reportadas para o time de Segurança da N26 Brasil.

1.6. Processos para contratação de fornecedores

Juntamente com o time de Compliance, o time de Segurança Cibernética realiza para todas as contratações, diligência específica para avaliar o risco da contratação submetendo os terceiros aos questionamentos sobre:

- ➔ estrutura de governança corporativa;
- ➔ capacidade do prestador em relação a infraestrutura tecnológica;
- ➔ cumprimento regulatório;
- ➔ acesso a dados e informações prestadas internamente e recuperação quando necessário;
- ➔ certificações quando exigido;
- ➔ relatórios de auditoria sobre os procedimentos concernentes à contratação;
- ➔ metodologia utilizada para gestão de acessos do produto contratado

Os fornecedores relevantes que prestam serviços de processamento e armazenamento de dados e de computação em nuvem são comunicados ao Banco Central, inclusive alterações contratuais, considerando a criticidade do serviço e a sensibilidade dos dados e das informações a serem processados, armazenados e gerenciados pelo contratado.

Os fornecedores relevantes possuem a obrigação de comunicar quaisquer incidentes que possam afetar diretamente as operações da N26 Brasil.

1.7. Treinamentos de segurança da informação

Os treinamentos sobre assuntos da segurança da informação serão realizados no mínimo duas vezes por ano, com assuntos livres dentro do âmbito da segurança da informação e serão criados e definidos pelo departamento de Engenharia.

Um plano de conscientização de segurança da informação é executado para garantir que a segurança da informação não seja apenas conhecida, mas compreendida por todos os colaboradores, conscientizando-os periodicamente sobre melhores práticas, requisitos mínimos, riscos e responsabilidades existentes e quais medidas devem ser adotadas quando houver incidentes de segurança de forma a atingir uma melhor utilização e proteção dos ativos de informação da N26 Brasil.

As principais diretrizes são:

- ➔ Organização de eventos que tenham o intuito de fortalecer a conscientização sobre diversos
- ➔ aspectos de segurança em geral (Sessões de compartilhamento).
- ➔ Divulgação de materiais e instruções relevantes (Cartilha de Segurança da Informação).

➔ Elaboração de um processo de treinamento continuado voltado à Segurança da Informação.

1.8. Contato

Em caso de dúvidas ou indício de incidente identificado pelo público em geral relacionado a segurança cibernética entre em contato pelo e-mail: **security@n26brasil.com.**

1.9. Glossário

Post-mortem: relatório feito depois de um incidente, contendo informações detalhadas e relevantes, como a causa raiz, linha do tempo de acontecimentos e próximos passos.

DLP: Data Loss Prevention, sistema para prevenção de vazamento de dados.

VPN: Virtual Private Network, rede virtual privada usada para acessar recursos internos.

SOC: Security Operations Center, central de operações de segurança que funciona 24x7x365.

PII: Personally Identifiable Information, informações pessoais que identificam pessoas de forma única, são considerados dados sensíveis.

n26brasil.com