

	POLÍTICA	Área responsável:	Segurança da Informação e Cibernética
		Elaborado em:	01/2026
		Revisado em:	07/2026
		Classificação da Informação:	Público
		Página(s):	1/26
		Tipo de Normativo:	Regulatório
		Cód. Do documento:	POL.SIC.001
		Rev.:	01
POLÍTICA DE SEGURANÇA DE INFORMAÇÃO E CIBERNÉTICA			

ÍNDICE

1	Objetivo	3
2	Aplicabilidade.....	3
3	Regulamentação, Legislação e Outros Documentos de referência	4
4	Termos e definições	5
5	Diretrizes	7
	5.1 Diretrizes sobre Dados e Informações em Ambiente Local e em Nuvem	8
	5.2 Contratação de Serviços de Processamento e Armazenamento de Dados e de Computação em Nuvem.....	9
	5.3 Diretriz de Gerenciamento de Segurança da Informação e Cibernética	11
	5.3.1 Controles técnicos obrigatórios de segurança cibernética.....	12
	5.4 Diretrizes para Cultura de Segurança da Informação e Cibernética	12
	5.5 Diretrizes em Caso de Violações de Dados e Incidentes de Segurança da Informação e Cibernética, e Avaliação da Relevância do Incidente.....	13
	5.5.1 Relatório anual sobre implementação do plano de ação e de resposta a incidentes cibernéticos	15
	5.6 Diretrizes de Gestão de Riscos de Segurança da Informação e Cibernética.....	16
	5.7 Gestão de Vulnerabilidades e Testes de Segurança	16
	5.8 Segurança de rede e infraestrutura.....	17
	5.9 Gestão de Certificados Digitais.....	17
	5.10 Segurança de Sistemas de Pagamentos e PIX.....	17
	5.11 Governança de Prevenção à Fraude	17
6	Responsabilidades	18
	6.1 Diretoria	18
	6.2 Diretoria de Serviços, Infraestrutura e Segurança	18
	6.3 Segurança da Informação	19
	6.4 Infraestrutura	20
	6.8 Gente e Gestão	22
	6.9 Treinamento e Desenvolvimento / Marketing	22
	6.8 Gerencias e Lideranças.....	22
	6.9 Colaboradores /Prestadores de Serviços	22

Cód. da Política:	Responsável(eis):	Revisão em:	Nº da Revisão:
POL. SIC.001	Segurança da Informação e Cibernética	07/2026	01

7 Disposições Gerais 23

7.1. Vigência e Aprovação 23

7.2. Consequências e Violações..... 23

8 Histórico..... 23

9 ANEXOS..... 24

Cód. da Política:	Responsável(eis):	Revisão em:	Nº da Revisão:
POL. SIC.001	Segurança da Informação e Cibernética	07/2026	01

1 Objetivo

Garantir a proteção e a manutenção da integridade, disponibilidade, confidencialidade e privacidade dos dados e de todas as informações sob responsabilidade da NDD Instituição de pagamento ("NDD Pay") e dos sistemas de informação utilizados, inclusive da computação em nuvem, além de contribuir para instituição de diretrizes que viabilizem a prevenção, detecção e redução de vulnerabilidades a incidentes relacionados com o ambiente cibernético.

2 Aplicabilidade

A Política de Segurança da Informação e Cibernética se aplica a todos os Administradores, Colaboradores, Parceiros e Fornecedores, responsáveis pela segurança cibernética da NDD Pay, que direta ou indiretamente utilizam ou suportam os sistemas, a infraestrutura ou as informações da instituição, e que devem, no que couber:

- Cumprir as normas e procedimentos relacionados ao uso de informações e sistemas associados, em conformidade com o estabelecido nesta Política;
- Informar, imediatamente, às áreas responsáveis, qualquer falha em dispositivo, serviço ou processo relacionado à Segurança da Informação e Segurança Cibernética, para que sejam tomadas ações de forma tempestiva;
- Utilizar as informações relacionadas à esta Política, como patrimônio da NDD Pay, e mantê-las seguras, integras e disponíveis, conforme sua classificação e necessidade.

Esta Política foi elaborada e revisada pelo Diretor responsável pela segurança da informação e cibernética, e aprovada pelos Administradores, e será revisada com a periodicidade mínima anual. A Política também poderá ser alterada, a qualquer momento, para contemplar quaisquer alterações regulatórias e outras obrigações legais.

Além da Política, o Diretor será responsável pela execução do plano de ação e de resposta a incidentes, que consiste em avaliar a política e os procedimentos de segurança da informação e cibernética adotados pela instituição.

Esta Política será compatível com:

- O porte, o perfil de risco e o modelo de negócio da NDD Pay;
- A natureza das atividades da NDD Pay e a complexidade dos seus produtos e serviços oferecidos; e
- A sensibilidade dos dados e das informações sob responsabilidade da instituição.

Cód. da Política:	Responsável(eis):	Revisão em:	Nº da Revisão:
POL. SIC.001	Segurança da Informação e Cibernética	07/2026	01

3 Regulamentação, Legislação e Outros Documentos de referência

Tipo	Emissor	Número	Ano	Assunto
Lei	Planalto	13.709	2018	Define princípios, bases legais e obrigações para o tratamento de dados pessoais. Exige medidas técnicas e administrativas adequadas para proteger dados pessoais. E obriga a notificação de incidentes de segurança que acarretaram vazamento de dados pessoais à ANPD (Agência Nacional de Proteção de Dados).
Decreto	Planalto	11.129	2022	Regulamenta a Lei nº 12.846, de 1º de agosto de 2013, que dispõe sobre a responsabilização administrativa e civil de pessoas jurídicas pela prática de atos contra a administração pública, nacional ou estrangeira.
Resolução	BCB	1	2020	Institui o arranjo de pagamentos Pix e aprova o seu Regulamento - Manual de Segurança.
Resolução	BCB	85	2021	Dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições de pagamento, pelas sociedades corretoras de títulos e valores mobiliários, pelas sociedades distribuidoras de títulos e valores mobiliários e pelas sociedades corretoras de câmbio autorizadas a funcionar pelo Banco Central do Brasil.
Resolução	BCB	80	2021	Estabelece os requisitos e os procedimentos para constituição e funcionamento, e de pedido de autorização de funcionamento das Instituições de Pagamento.
Resolução	BCB	198	2022	Dispõe sobre o requerimento mínimo de Patrimônio de Referência de Instituição de Pagamento (PRIP) de conglomerado do Tipo 2, nos termos da Resolução BCB nº 197, de 11 de março de 2022, e de instituição de pagamento não integrante de conglomerado prudencial, e sobre a metodologia de apuração desses requerimentos e a respectiva estrutura de gerenciamento contínuo de riscos.
Resolução	BCB	260	2022	Dispõe sobre os sistemas de controles internos das administradoras de consórcio, das instituições de pagamento, das sociedades corretoras de títulos e valores mobiliários, das sociedades distribuidoras de títulos e valores mobiliários e das sociedades corretoras de câmbio autorizadas a funcionar pelo Banco Central do Brasil.

Cód. da Política:	Responsável(eis):	Revisão em:	Nº da Revisão:
POL. SIC.001	Segurança da Informação e Cibernética	07/2026	01

Resolução	BCB	538	2025	A Resolução BCB nº 538/2025 atualiza e fortalece a Resolução BCB nº 85/2021, ampliando os requisitos de segurança cibernética aplicáveis às instituições autorizadas pelo Banco Central, incluindo instituições de pagamento.
Política	NDD Pay	-	2026	Política de Privacidade de Dados Pessoais
Procedimento	NDD Pay	-	2026	Procedimento de resposta a incidentes de segurança da informação e/ou cibernético

Em caso de conflitos entre as normas desta demais políticas, ou dúvida, contate a Área de [Compliance] da NDD Pay.

4 Termos e definições

- **Ativos Tecnológicos:** No contexto de Segurança da Informação, é qualquer bem ou direito que tenha valor para a Instituição, como computadores, dispositivos móveis, sistemas, aplicativos, bases de dados, informações, sala de servidores, entre outros.
- **Banco Central do Brasil (Bacen ou BCB):** Autarquia federal de natureza especial, autônoma, que tem como função, entre outras, regulamentar o funcionamento instituições financeiras, instituições de pagamento, dentre outras instituições.
- **Colaboradores:** São considerados colaboradores todas as pessoas físicas ou jurídicas que mantenham ou tenham mantido qualquer tipo de vínculo com a NDD Instituição de Pagamento S.A. (NDD Pay), incluindo, mas não se limitando a: empregados, aprendizes, estagiários, prestadores de serviço, diretores, administradores, sócios que venham a ter acesso a informações da NDD Pay e/ou que utilizem, venham a utilizar ou tenham utilizado sua infraestrutura tecnológica, ainda que já encerrado o vínculo contratual ou jurídico anteriormente existente.
- **Terceiros:** Prestadores de serviço, sejam essas quaisquer empresas ou pessoas jurídicas que possam prestar serviço para a NDD Pay.
- **Parceiros de Negócio:** São empresas ou profissionais externos que possuem relação contratual com a organização e necessitam acessar informações, sistemas ou serviços para realizar entregas ou suporte. Seu acesso deve ser limitado ao estritamente necessário, controlado e monitorado, respeitando as políticas de segurança, cláusulas contratuais e obrigações de confidencialidade.
- **Confidencialidade:** Garantir que as informações tratadas sejam de conhecimento exclusivo de pessoas especificamente autorizadas.
- **Comitê de Crise:** Composto por ao menos um representante de cada uma das seguintes áreas: Segurança da Informação, Infraestrutura e Privacidade de Dados, juntamente com o Diretor de Serviços e Operações;
- **Dado:** Para os fins desta Política, dado é o registro do atributo de um ente, objeto ou fenômeno onde

Cód. da Política:	Responsável(eis):	Revisão em:	Nº da Revisão:
POL. SIC.001	Segurança da Informação e Cibernética	07/2026	01

registro significa a gravação ou a impressão de caracteres ou símbolos que tenham um significado em algum documento ou suporte físico.

- **Dado em nuvem:** Dado armazenado em servidores de alta disponibilidade via internet.
- **Dado em repouso:** Dado armazenado em computador, servidor, drive externo, dispositivo móvel, e outros que não o movimento de um local para outro.
- **Dado Produtivo:** Dados utilizados no ambiente de produção.
- **Dados Pessoais:** quaisquer informações relativas a uma pessoa natural ("Titular" ou Titular dos Dados"), que possibilite sua identificação individualizada; em especial por referência a um identificador único; como por exemplo, nome, número de identificação ou documento oficial, dados de localização, identificadores eletrônicos, ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, econômica, cultural ou social do titular, ou ainda a combinação de mais de um destes dados.
- **Dados Pessoais Sensíveis:** informações sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculados a uma pessoa natural.
- **Disponibilidade:** Garantir que as informações estejam disponíveis a todas as pessoas autorizadas a tratá-las.
- **Duplo fator de autenticação:** É um recurso que acrescenta uma camada adicional de segurança para o processo de login da conta, exigindo que o usuário forneça duas formas de autenticação.
- **Falhas de Segurança:** São vulnerabilidades que podem gerar indisponibilidade ou comprometer a segurança dos sistemas.
- **Fornecedores Críticos:** Um fornecedor é considerado crítico nas situações em que o descumprimento de um determinado critério relacionado à contratação pode impactar significativamente o negócio ou as atividades da Instituição.
- **Incidentes Relevantes:** São incidentes capazes de causar risco ou dano relevante para o negócio (exemplos: dados financeiros, contábeis, gerenciais) e, aqueles que possam causar danos materiais ou morais aos titulares.
- **Integridade:** Garantir que as informações sejam mantidas íntegras, sem modificações indevidas – acidentais ou propositais.
- **Privacidade e Proteção de Dados:** Responsabilidade nas atividades de tratamento de Dados Pessoais, seguindo os preceitos estabelecidos pela Lei Geral de Proteção de Dados (Lei nº 13.709/18), tais como finalidade, necessidade, transparência, segurança e não discriminação.
- **Risco cibernético:** Possibilidade de perdas financeiras, operacionais, legais, de imagem ou de conformidade decorrentes de incidentes em ambiente digital/tecnológico.

Cód. da Política:	Responsável(eis):	Revisão em:	Nº da Revisão:
POL. SIC.001	Segurança da Informação e Cibernética	07/2026	01

- **Segurança Cibernética:** Conjunto de práticas, processos, tecnologias e controles usados para proteger sistemas, redes, dispositivos, dados e usuários contra-ataques, acessos não autorizados, danos, uso indevido ou interrupções no ambiente digital.
- **Segurança da Informação:** Protege a informação em qualquer formato (digital, papel, verbal, físico etc.) contra acesso, uso, divulgação, alteração ou destruição não autorizados. É baseada nos pilares: Confidencialidade, Integridade, Disponibilidade e Autenticidade/Rastreabilidade.
- **Sistema da Informação:** Um conjunto organizado de elementos, podendo ser pessoas, dados, atividades ou recursos materiais em geral. Estes elementos interagem entre si para processar informação e divulgá-la de forma adequada em função dos objetivos de uma organização.
- **Transação(ões):** para fins desta Política, consistem nas movimentações realizadas pelo Cliente de sua conta de pagamento, mediante o aporte, a transferência ou o resgate de recursos financeiros.
- **Vazamento de Dados Pessoais:** consiste na violação dos dados pessoais e/ou dados pessoais sensíveis que são indevidamente acessados, coletados e divulgados na internet, por meio da invasão de sistemas de uma organização, por terceiros não autorizados.

5 Diretrizes

Toda informação, registro, documento ou dado produzido, coletado, recebido, processado ou mantido sob responsabilidade da NDD Pay é considerado patrimônio da Instituição, devendo ser utilizado exclusivamente para fins corporativos legítimos.

Os dados representam informações e, portanto, configuram-se como ativos estratégicos de elevado valor e relevância para a Instituição, constituindo elemento essencial para a continuidade do negócio e para a tomada de decisão gerencial.

A coleta, o tratamento, o armazenamento, o acesso, a transferência e/ou o compartilhamento de dados pertencentes à Instituição, por colaboradores, prestadores de serviço, fornecedores, parceiros comerciais, administradores ou acionistas, devem observar rigorosamente as diretrizes estabelecidas nesta Política e nos demais normativos internos aplicáveis, incluindo políticas, normas, procedimentos operacionais e manuais correlatos.

De forma geral, é vedada a divulgação de dados ou informações institucionais a pessoas não autorizadas, inclusive no ambiente interno. Qualquer divulgação externa somente poderá ocorrer mediante autorização prévia e formal da NDD Pay, devendo ser registrada e controlada, com identificação clara do repositório de armazenamento e do responsável pelo tratamento, de modo a permitir rastreabilidade e pronta disponibilização ao Banco Central do Brasil, quando solicitada.

Cód. da Política:	Responsável(eis):	Revisão em:	Nº da Revisão:
POL. SIC.001	Segurança da Informação e Cibernética	07/2026	01

Para garantir a conformidade com estas diretrizes, são implementados controles e salvaguardas de segurança destinados a prevenir o uso indevido, o acesso não autorizado, o vazamento, a alteração ou a destruição indevida de dados pessoais, dados sensíveis e demais informações institucionais, bem como a proteger a infraestrutura tecnológica da NDD Pay contra ameaças internas e externas.

A NDD Pay assegura que todos os seus colaboradores, prestadores de serviço, parceiros de negócios e terceiros adotem práticas que garantam a confidencialidade, a integridade e a disponibilidade das informações sob sua guarda ou acesso, nos termos da Resolução BCB nº 85/2021.

Considerando a dinâmica de evolução tecnológica e o cenário crescente de ameaças cibernéticas, é responsabilidade de cada colaborador cumprir integralmente as orientações e mecanismos de proteção homologados pela área de Segurança da Informação, adotando todas as medidas cabíveis para resguardar as informações corporativas, ainda que determinadas situações específicas não estejam expressamente previstas nesta Política.

5.1 Diretrizes sobre Dados e Informações em Ambiente Local e em Nuvem

- O acesso a dados e informações deve ser estritamente restrito e controlado, devendo ser implementados mecanismos de segurança que assegurem que tais informações sejam consultadas, modificadas, armazenadas ou manipuladas exclusivamente por pessoas devidamente autorizadas, conforme seus perfis de acesso e responsabilidades funcionais.
- Todos os colaboradores da NDD Pay devem formalizar, no momento de sua admissão, a Cláusula de Confidencialidade e Sigilo no Contrato de Trabalho, bem como aceitar o Termo de Uso de Sistemas Internos da NDD Pay, renovando este último anualmente ou sempre que houver atualização, garantindo a aderência contínua às diretrizes de proteção de informações da Instituição.
- Os ativos de informação vinculados à geração, armazenamento, comunicação e processamento de dados devem ser inventariados e controlados, com identificação de seus responsáveis e respectivas finalidades de uso, de modo a assegurar rastreabilidade, governança e proteção adequada.
- A utilização de ativos de informação, recursos tecnológicos e sistemas corporativos deve ocorrer mediante autorização prévia e restrita às finalidades profissionais necessárias para o exercício das atividades do colaborador, sendo vedado o uso para propósitos pessoais ou não autorizados.
- O responsável pela informação deve adotar os controles de segurança aplicáveis e compatíveis com o nível de criticidade e classificação da informação (pública, interna ou confidencial), garantindo proteção adequada durante todo o ciclo de vida do dado.
- A criação, armazenamento, processamento e compartilhamento de dados em ambiente de computação em nuvem devem ser previamente aprovados pela área responsável, devidamente

Cód. da Política:	Responsável(eis):	Revisão em:	Nº da Revisão:
POL. SIC.001	Segurança da Informação e Cibernética	07/2026	01

monitorados, controlados e registrados pela NDD Pay, observando requisitos de segurança, localização, privacidade e conformidade normativa.

5.2 Contratação de Serviços de Processamento e Armazenamento de Dados e de Computação em Nuvem

Antes da celebração de contratos para prestação de serviços de processamento ou armazenamento de dados e de computação em nuvem, a NDD Pay deve avaliar, validar, registrar e manter evidências acerca da capacidade técnica, operacional e de conformidade do potencial prestador de serviços, assegurando que este garanta:

- O acesso da Instituição às informações que serão processadas, tratadas ou armazenadas pelo prestador de serviços;
- A confidencialidade, a integridade, a disponibilidade, a autenticidade e a recuperabilidade dos dados e informações;
- A aderência do prestador às certificações técnicas e controles de segurança exigidos pela NDD Pay;
- A conformidade com a legislação brasileira aplicável, especialmente a Lei Geral de Proteção de Dados – LGPD (Lei nº 13.709/2018);
- O acesso da NDD Pay a relatórios de auditoria independente que avaliem os controles internos e procedimentos de segurança do prestador de serviços;
- A disponibilização de informações e meios que permitam o monitoramento contínuo do serviço contratado;
- A segregação lógico-física dos dados da NDD Pay em relação aos dados de outros clientes do prestador de serviços;
- A efetividade dos controles de acesso implementados para proteção das informações da Instituição e de seus usuários finais.

A avaliação de risco e relevância do serviço a ser contratado deverá ser realizada pela área contratante, com apoio da Área de Segurança da Informação e Cibernética e, quando aplicável, das Áreas de *Compliance*, Gestão de Riscos e Controles Internos, considerando:

- A criticidade do serviço;
- A sensibilidade das informações envolvidas;
- A classificação das informações tratadas;
- A dependência operacional do serviço contratado; e
- O potencial impacto sobre a continuidade do negócio.

Nos termos da regulamentação vigente, a contratação de serviços de computação em nuvem compreende, no mínimo, a disponibilização à NDD Pay de um ou mais dos seguintes serviços:

Cód. da Política:	Responsável(eis):	Revisão em:	Nº da Revisão:
POL. SIC.001	Segurança da Informação e Cibernética	07/2026	01

I – Processamento de dados, armazenamento de informações, infraestrutura tecnológica, redes e demais recursos computacionais necessários para operação de sistemas e aplicações;

II – Execução ou implantação de *softwares* próprios ou de terceiros, utilizando infraestrutura do prestador de serviços;

III – Execução de aplicações diretamente via internet, com recursos computacionais do prestador de serviços.

A NDD Pay deverá adotar mecanismos que garantam que a prestação dos serviços contratados observe integralmente as exigências da Resolução BCB nº 85/2021, bem como demais normas aplicáveis, assegurando:

- Governança e rastreabilidade;
- Segurança cibernética;
- Proteção e privacidade de dados;
- Continuidade operacional;
- Resiliência tecnológica.

Sempre que houver contratação de serviços relevantes de processamento de dados, armazenamento ou computação em nuvem, a Área de Regulatório e PLD/FT deverá comunicar o Banco Central do Brasil no prazo de até 10 (dez) dias úteis, contendo:

- I. A razão social do prestador contratado;
- II. A descrição dos serviços relevantes contratados;
- III. A indicação do país e da região onde os dados poderão ser armazenados, processados ou gerenciados.

Parágrafo único: Alterações contratuais que modifiquem o objeto do serviço contratado também devem ser comunicadas ao Banco Central do Brasil no mesmo prazo acima mencionado.

A contratação de serviços relevantes prestados no exterior deve observar integralmente os requisitos da Resolução BCB nº 85/2021, especialmente quanto à governança de riscos, soberania dos dados e capacidade de supervisão pelo regulador.

Os contratos firmados pela NDD Pay para prestação de serviços relevantes de computação em nuvem devem conter cláusulas que tratem, obrigatoriamente, sobre:

- I. Localidade dos dados (país e região);
- II. Medidas de segurança adotadas para transmissão, tratamento e armazenamento das informações;
- III. Segregação de dados e controle de acessos;
- IV. Condições de término contratual, contemplando:
 - a) transferência segura dos dados à NDD Pay ou a novo fornecedor;
 - b) exclusão definitiva dos dados após transferência, com emissão de declaração formal.

Cód. da Política:	Responsável(eis):	Revisão em:	Nº da Revisão:
POL. SIC.001	Segurança da Informação e Cibernética	07/2026	01

V. Privacidade de dados pessoais, nos casos em que haja tratamento de dados pessoais ou sensíveis.

Disposição final: Todos os contratos de prestação de serviços da NDD Pay devem observar estritamente a legislação e regulamentação vigente, devendo ser previamente avaliados e aprovados pela Área Jurídica, com suporte das áreas de Segurança da Informação; *Compliance*, PLD e Riscos, quando aplicável.

5.3 Diretriz de Gerenciamento de Segurança da Informação e Cibernética

O gerenciamento dos controles de segurança da informação e cibernética deve assegurar que os procedimentos operacionais sejam planejados, implementados, monitorados e continuamente aprimorados, em conformidade com os princípios, diretrizes e responsabilidades definidos nesta Política.

Esses controles devem garantir a efetividade do Sistema de Gestão de Segurança da Informação (SGSI) e a resiliência operacional da NDD Pay, em aderência à Resolução BCB nº 85/2021.

I. A gestão de segurança deve contemplar:

- avaliação e tratamento contínuo de riscos de segurança da informação e cibernética;
- adoção de controles preventivos, detectivos e corretivos;
- definição clara de papéis e responsabilidades;
- rastreabilidade das ações e dos acessos;
- proteção dos ativos de informação críticos ao negócio;
- integração com os planos de continuidade de negócios e de resposta a incidentes.

II. Comunicação de Incidentes Relevantes

Nos casos de incidentes de segurança considerados relevantes, conforme critérios de classificação previstos neste documento (Item 5.5), a NDD Pay deve:

- notificar tempestivamente o Banco Central do Brasil, conforme prazos e critérios definidos na regulamentação aplicável;
- notificar tempestivamente os clientes e em até 48 horas após o conhecimento do incidente de segurança da informação com vazamento de dados pessoais a ANPD – Agência Nacional Proteção de dados;
- compartilhar informações essenciais sobre o incidente, quando necessário, com outras instituições de pagamento ou instituições autorizadas a funcionar pelo Banco Central, respeitando o sigilo empresarial e a legislação vigente;
- cooperar com autoridades regulatórias em eventuais investigações ou solicitações de informações;
- registrar as evidências, analisar causas-raiz e implementar ações de correção e prevenção.

III. Rastreabilidade das transações e operações realizadas

Cód. da Política:	Responsável(eis):	Revisão em:	Nº da Revisão:
POL. SIC.001	Segurança da Informação e Cibernética	07/2026	01

A NDD Pay deve garantir a rastreabilidade completa das transações e operações realizadas em seus sistemas, incluindo:

- geração e retenção de logs de auditoria fim a fim;
- identificação de falhas, comportamentos atípicos e tentativas de fraude;
- definição de prazos de retenção conforme criticidade dos dados;
- armazenamento seguro das trilhas de auditoria.

Os registros devem permitir reconstrução de eventos e suporte a investigações internas e externas.

5.3.1 Controles técnicos obrigatórios de segurança cibernética

Em conformidade com a Resolução BCB nº 85/2021, com redação atualizada pela Resolução BCB nº 538/2025, a NDD Pay deve implementar e manter controles técnicos mínimos obrigatórios de segurança cibernética, abrangendo:

- Mecanismos de autenticação, incluindo autenticação multifator (MFA) para acessos críticos e remotos;
- Uso de criptografia para proteção de dados em trânsito e em repouso;
- Mecanismos de prevenção e detecção de intrusão (IDS/IPS);
- Mecanismos de prevenção de vazamento de dados (DLP);
- Proteção contra softwares maliciosos (antimalware/EDR);
- Mecanismos de rastreabilidade de operações e acessos;
- Gestão de backups com garantia de integridade e recuperação;
- Processos contínuos de identificação, avaliação e correção de vulnerabilidades;
- Controles de acesso baseados no princípio do menor privilégio;
- Definição de padrões seguros de configuração de ativos tecnológicos;
- Mecanismos de proteção de rede;
- Gestão de certificados digitais;
- Segurança na integração de sistemas via APIs ou interfaces eletrônicas;
- Monitoramento ativo de ameaças cibernéticas, incluindo deep web e dark web.

Esses controles devem ser aplicados tanto no ambiente interno quanto em sistemas desenvolvidos ou operados por terceiros.

5.4 Diretrizes para Cultura de Segurança da Informação e Cibernética

A NDD Pay deve promover e consolidar uma cultura organizacional de segurança cibernética, alinhada aos princípios de responsabilidade, prevenção, conformidade regulatória e proteção de dados. Para isso, deve assegurar que todos os colaboradores, administradores, terceirizados e parceiros estratégicos atuem de forma consciente e responsável no tratamento das informações e dos ativos tecnológicos da Instituição.

Cód. da Política:	Responsável(eis):	Revisão em:	Nº da Revisão:
POL. SIC.001	Segurança da Informação e Cibernética	07/2026	01

Para garantir esse propósito, a NDD Pay deve:

- Disponibilizar e comunicar de forma clara e tempestiva todas as políticas, normas internas, procedimentos operacionais e manuais relacionados à Segurança Cibernética e Segurança da Informação para todos os colaboradores, prestadores de serviço relevantes e terceiros autorizados;
- Publicar e manter acessível em seu sítio eletrônico institucional o “Anexo I – Recomendações e Instruções de Segurança Cibernética para Clientes e Usuários”, garantindo ampla divulgação e orientação aos clientes, parceiros e demais partes interessadas;
- Realizar treinamentos obrigatórios de segurança cibernética ao menos uma vez ao ano para todos os colaboradores, bem como treinamentos adicionais sempre que houver atualização significativa desta Política ou mudanças relevantes no ambiente de ameaças cibernéticas;
- Conduzir campanhas permanentes de conscientização em segurança da informação e cibersegurança, com foco em prevenção de incidentes, proteção de dados, boas práticas digitais e conformidade normativa;
- Reportar periodicamente à Diretoria os indicadores de evolução, desempenho e aderência dos programas de capacitação e conscientização em segurança cibernética, garantindo o acompanhamento estratégico da alta administração.

5.5 Diretrizes em Caso de Violações de Dados e Incidentes de Segurança da Informação e Cibernética, e Avaliação da Relevância do Incidente

A NDD Pay deve adotar mecanismos eficazes para identificação, tratamento, registro e comunicação de incidentes de segurança da informação e cibersegurança, observando os princípios de prevenção, resposta tempestiva e redução de impactos, conforme diretrizes da Resolução BCB nº 85/2021 e demais normativos aplicáveis.

Além disso, a NDD Pay deve definir critérios formais para caracterização de situação de crise, considerando:

- Indisponibilidade de serviços críticos;
- Impacto financeiro relevante;
- Vazamento de dados sensíveis;
- Comprometimento da confiança de clientes;
- Impacto no Sistema Financeiro Nacional.

Esses critérios devem ser documentados e utilizados para acionamento do plano de continuidade.

I. Comunicação e Registro de Incidentes

- É obrigação de todo colaborador, prestador de serviços ou terceiro autorizado comunicar imediatamente à Área de Segurança da Informação qualquer evento, indício, falha, vulnerabilidade,

Cód. da Política:	Responsável(eis):	Revisão em:	Nº da Revisão:
POL. SIC.001	Segurança da Informação e Cibernética	07/2026	01

anomalia ou situação que possa comprometer a confidencialidade, integridade, disponibilidade ou autenticidade de dados, informações ou sistemas da Instituição. A comunicação deve ocorrer por meio dos canais oficiais estabelecidos pela NDD Pay, conforme definido no Procedimento de Resposta a Incidentes de Segurança da Informação e Cibernético.

- Toda suspeita ou confirmação de incidente de segurança deve ser avaliada de forma estruturada pela Área de Segurança da Informação, incluindo, entre outros, os seguintes cenários:
 - Acesso não autorizado, acidental ou ilícito;
 - Destruição, alteração, perda ou vazamento de dados;
 - Falhas de integridade em sistemas e bases de dados;
 - Indisponibilidade ou interrupção de serviços críticos;
 - Uso indevido de credenciais ou acessos privilegiados; e
 - Qualquer forma inadequada ou ilícita de tratamento de dados.

II. Avaliação de Relevância do Incidente

A avaliação deve considerar potenciais impactos tais como:

- a) Risco aos direitos e liberdades de titulares de dados;
- b) Risco reputacional à Instituição;
- c) Risco financeiro ou operacional;
- d) Risco regulatório e legal;
- e) Outros riscos relevantes ao negócio.

Atenção: Quando houver suspeita ou confirmação de incidente envolvendo Dados Pessoais ou Dados Pessoais Sensíveis, a Área de Privacidade (DPO) deve ser acionada imediatamente através do e-mail dpo@nddip.com.br em conformidade com a LGPD (Lei nº 13.709/2018).

III. Atuação e Governança na Resposta

Os resultados da investigação devem ser documentados e reportados à Diretoria, contendo:

- Descrição do incidente (data, horário e origem);
- Ativos e sistemas afetados;
- Dados potencialmente comprometidos;
- Impacto avaliado;
- ações corretivas adotadas;
- plano de mitigação;
- responsáveis pela execução das ações;
- eventuais comunicações ao regulador e autoridades.

Cód. da Política:	Responsável(eis):	Revisão em:	Nº da Revisão:
POL. SIC.001	Segurança da Informação e Cibernética	07/2026	01

Nota: Essas informações devem compor o Relatório Anual com Plano de Resposta a Incidentes de Segurança Cibernética previsto na regulamentação (Resolução BCB nº 85/2021, Art. 25).

- Havendo potencial impacto relevante ao Sistema Financeiro Nacional (SFN) ou Sistema de Pagamentos Brasileiro (SPB), a NDD Pay deve comunicar imediatamente o Banco Central do Brasil dentro dos prazos regulamentares.

IV. Medidas de Preservação de Evidências e Colaboração

- Durante a apuração de incidente, a Área de Segurança da Informação poderá, sempre que necessário e sem aviso prévio, recolher dispositivos corporativos ou restringir acessos para garantir a preservação de evidências e a continuidade da investigação.
- Em incidentes envolvendo dados pessoais, o Encarregado de Dados (DPO) deve acompanhar todo o processo, inclusive eventuais notificações à Autoridade Nacional de Proteção de Dados (ANPD) e aos titulares, quando aplicável.

5.5.1 Relatório anual sobre implementação do plano de ação e de resposta a incidentes cibernéticos

O plano de ação e de resposta a incidentes cibernéticos deve visar à implementação da Política de Segurança da Informação e Cibernética, abrangendo:

- I) as ações a serem desenvolvidas para adequar as estruturas organizacionais e operacionais aos princípios e às diretrizes da presente política;
- II) as rotinas, os procedimentos, os controles e as tecnologias a serem utilizados na prevenção e na resposta a incidentes, em conformidade com as diretrizes desta política; e
- III) a área responsável pelo registro e controle dos efeitos de incidentes relevantes.

O Relatório anual sobre a implementação do plano de ação e de resposta a incidentes deverá ser elaborado com a data base de 31 de dezembro e abordar, no mínimo, os seguintes pontos:

- a) a efetividade da implantação das ações relacionadas à adequação da estrutura organizacional e operacional da Instituição aos princípios e diretrizes desta Política;
- b) o resumo dos resultados obtidos na implantação das rotinas, dos procedimentos, dos controles e das tecnologias utilizados na prevenção e na resposta a incidentes;
- c) os incidentes relevantes ocorridos, relacionados com o ambiente cibernético, contendo, no mínimo, as seguintes informações: tipo de incidente, data e hora, ações remediadoras, área responsável pela tratativa, áreas afetadas e avaliação de impacto, e, ainda, as rotinas, procedimentos, controles e tecnologias utilizados na prevenção e na resposta de novos incidente, área responsável pelo registro e

Cód. da Política:	Responsável(eis):	Revisão em:	Nº da Revisão:
POL. SIC.001	Segurança da Informação e Cibernética	07/2026	01

controle dos efeitos de incidentes relevantes, descrição se houve vazamento de dados e relevância dos dados e do incidente.

d) os resultados dos testes de continuidade dos serviços de pagamento prestados, considerando cenários de indisponibilidade ocasionada por incidentes; e

e) previsão de período para verificação de eficácia do plano de ação implementado.

Em conformidade com a regulamentação em vigor, o Relatório deve ser apresentado à Diretoria, até 31 de março do ano seguinte ao da data-base.

5.6 Diretrizes de Gestão de Riscos de Segurança da Informação e Cibernética

A NDD Pay deve adotar práticas estruturadas e contínuas para identificação, avaliação, tratamento e monitoramento de riscos de segurança cibernética, visando proteger seus ativos tecnológicos, garantir a continuidade de suas operações e preservar a integridade, confidencialidade e disponibilidade das informações críticas.

Assim, ficam estabelecidas as seguintes diretrizes:

- É responsabilidade da Área de Segurança da Informação, com apoio da Área de Gestão de Riscos, identificar e avaliar os riscos cibernéticos associados aos ativos de tecnologia e processos da NDD Pay. Os resultados das avaliações devem ser formalmente documentados e reportados à Diretoria de Tecnologia e, posteriormente, à Diretoria para deliberação e acompanhamento.
- Todo desenvolvimento, aquisição, contratação, implementação ou alteração relevante de sistemas e soluções tecnológicas que envolvam tratamento, armazenamento ou transmissão de dados institucionais deve passar por análise formal de risco conduzida pela Área de Segurança da Informação. A execução somente poderá ocorrer mediante aprovação prévia da Diretoria, especialmente quando envolver dados sensíveis, estratégicos ou dados pessoais, em conformidade com a legislação e regulamentação vigente.
- O tratamento dos riscos identificados deve ser conduzido pelas áreas responsáveis pelos ativos, processos ou soluções avaliadas, sob coordenação da Diretoria de Tecnologia e supervisão da Área de Segurança da Informação. O status das ações corretivas ou mitigatórias deve ser monitorado e periodicamente reportado à Diretoria, até a mitigação dos riscos ou aceitação formal do risco residual.

5.7 Gestão de Vulnerabilidades e Testes de Segurança

A NDD Pay deve implementar processo contínuo de gestão de vulnerabilidades, incluindo:

- Varreduras periódicas automatizadas;
- Testes de intrusão (pentests) com periodicidade mínima anual;

Cód. da Política:	Responsável(eis):	Revisão em:	Nº da Revisão:
POL. SIC.001	Segurança da Informação e Cibernética	07/2026	01

- Análises técnicas independentes;
- Correção tempestiva das vulnerabilidades identificadas.

Os testes devem ser realizados por entidade independente ou equipe interna segregada, com documentação formal dos resultados e planos de ação.

5.8 Segurança de rede e infraestrutura

A NDD Pay deve implementar controles de segurança de rede que incluam, no mínimo:

- Segmentação de rede, isolando ambientes críticos;
- Uso de firewalls e monitoramento de conexões;
- Controle de acessos externos;
- Uso de VPN segura para acessos remotos;
- Detecção de comportamentos anômalos em rede;
- Restrição de acesso a dispositivos autorizados.

Deve ser garantida proteção reforçada para ambientes produtivos e sistemas críticos.

5.9 Gestão de Certificados Digitais

A NDD Pay deve assegurar a gestão segura de certificados digitais, incluindo:

- Monitoramento do uso de certificados;
- Controle rigoroso de acesso às chaves privadas;
- Prevenção de compartilhamento indevido;
- Validação contínua de certificados revogados.

O acesso a chaves privadas deve ser restrito e auditável.

5.10 Segurança de Sistemas de Pagamentos e PIX

Conforme resolução BCB n. 538/2025, para atuação em sistemas do Sistema de Pagamentos Brasileiro (SPB), incluindo PIX, a NDD Pay deve:

- Implementar autenticação multifator para acessos administrativos;
- Garantir isolamento lógico e físico dos ambientes PIX;
- Monitorar uso de credenciais e certificados;
- Validar a integridade das transações antes da assinatura digital;
- Impedir acesso de terceiros às chaves privadas utilizadas em transações;
- Implementar controles antifraude específicos para operações financeiras.

5.11 Governança de Prevenção à Fraude

A NDD Pay deve definir, monitorar e reportar métricas de segurança cibernética, incluindo:

Cód. da Política:	Responsável(eis):	Revisão em:	Nº da Revisão:
POL. SIC.001	Segurança da Informação e Cibernética	07/2026	01

- Número de incidentes de segurança;
- Tempo médio de resposta a incidentes (MTTR);
- Quantidade de vulnerabilidades identificadas e corrigidas;
- Percentual de aderência a controles de segurança;
- Eficácia de testes de continuidade e intrusão;
- Indicadores de fraude e tentativas bloqueadas.

Os indicadores devem ser reportados periodicamente à Diretoria e utilizados para melhoria contínua.

6 Responsabilidades

6.1 Diretoria

- Avaliar e aprovar a presente Política, conforme norma vigente;
- Assegurar que a Política de Segurança da Informação e Cibernética e os objetivos de segurança cibernética estão estabelecidos e são compatíveis com a direção estratégica da organização;
- Garantir que os recursos necessários para o sistema de gestão da segurança cibernética estão disponíveis;
- Promover a cultura de segurança cibernética e da conformidade com os requisitos do sistema de gestão da segurança cibernética;
- Autorizar as exceções da presente política.

6.2 Diretoria de Serviços, Infraestrutura e Segurança

- Definir diretrizes relacionadas à segurança da informação e cibernética;
- Instituir planos de ação e definir respostas a possíveis incidentes de segurança, conforme Procedimento de Resposta de Incidentes de Segurança da Informação e Cibernético;
- Instituir, sempre que necessário e/ou demandado pela Diretoria, instrumentos de controle de violações às diretrizes aqui estabelecidas;
- Treinar, com o apoio da área de gestão de pessoas, todos os colaboradores, e conscientizá-los acerca das diretrizes e regulamentos de Segurança Cibernética e Segurança da Informação;
- Reportar à Diretoria qualquer tipo de incidente e/ou violações relacionadas à presente política, assim como os planos de recuperação após incidente cibernético;
- Notificar, tempestivamente, às áreas de *Compliance* e/ou Controles Internos, as ocorrências de incidentes relevantes e interrupções dos serviços relevantes, que configurem situação de crise pela Instituição, bem como das providências para o reinício das suas atividades, que devem ser comunicados ao BACEN;
- Compartilhar, tempestivamente, com as instituições de pagamento e demais instituições autorizadas a funcionar pelo Banco Central, os incidentes relevantes;

Cód. da Política:	Responsável(eis):	Revisão em:	Nº da Revisão:
POL. SIC.001	Segurança da Informação e Cibernética	07/2026	01

- Implantar mecanismo ou instrumento para viabilizar o compartilhamento de informações sobre incidentes relevantes com as instituições de pagamento e demais instituições autorizadas a funcionar pelo Banco Central;
- Informar, às áreas de *Compliance* e Controles Internos, a relação de fornecedores relevantes contratados, que deverão ser comunicados ao BACEN, em até 5 (cinco) dias da data da contratação;
- Propor e, quando necessário, conduzir a execução de ações corretivas ou preventivas pertinentes a qualquer matéria relacionada à segurança da informação e cibernética;
- Notificar, tempestivamente, o DPO, as ocorrências de incidentes de segurança da informação que envolvam dados pessoais, bem como as áreas de *Compliance* e Controles Internos;
- Informar, nos casos de incidentes que envolvam dados pessoais, quais dados pessoais foram afetados, os titulares envolvidos e as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo;
- Assegurar a governança dos dados, a fim de garantir a confidencialidade, disponibilidade e integridade das informações;
- Aplicar o princípio do privilégio mínimo de acesso a todas as solicitações, condicionando a concessão de acesso à necessidade efetiva e, ainda, considerando anonimização de dados sensíveis;

6.3 Segurança da Informação

- Viabilizar e operacionalizar todos os mecanismos e/ou instrumentos necessários a aplicabilidade desta política;
- Garantir que todos os recursos necessários à aplicação da presente política sejam disponibilizados;
- Analisar a documentação e os controles implementados validando a aderência dos controles da política.
- Propor a implementação de novos controles a fim de aderência regulatória e aumento de maturidade de segurança da informação.
- Checar a eficácia e efetividade dos mecanismos instituídos/implantados, pela Instituição, para garantir a segurança cibernética;
- Monitorar periodicamente a efetividade da aplicação da presente política, por meio de reporte das áreas operacionais e, ainda, quando possível, pela execução de Avaliações de Controles de Segurança da Informação;
- Desenvolver, implantar e/ou aprimorar as soluções de tecnologia, relacionadas à Segurança da Informação;
- Orientar o controle do antivírus/*antimalware* em todos os servidores, estações de trabalho e notebooks;
- Garantir a Salvaguarda da licença de uso do antivírus;

Cód. da Política:	Responsável(eis):	Revisão em:	Nº da Revisão:
POL. SIC.001	Segurança da Informação e Cibernética	07/2026	01

- Monitorar constante as eventuais vulnerabilidades técnicas dos ativos de informação;
- Aplicar testes de intrusão periódicos (pentest);
- Aplicar controles e procedimentos para correção das vulnerabilidades identificadas, incluindo a proteção contra a instalação de softwares maliciosos;
- Implantar controles visando a prevenção a vazamento de dados;
- Estabelecer conexões de acesso remoto rastreáveis por meio de trilhas de auditoria;
- Implantar controles para garantir que as informações sejam conhecidas, alteradas e acessadas somente por pessoas autorizadas, e constar tal diretriz em Política de Classificação das Informações;
- Avaliar, em conjunto com *Compliance*, os riscos inerentes a segurança cibernética nos ativos de tecnologia da informação da NDD Pay e reportá-los à Diretoria de Serviços, Infraestrutura e segurança;
- Apoiar a Área de Tecnologia da Informação nas ações que garantam a continuidade de negócios.

6.4 Infraestrutura

- Gerenciar, descrever e testar, com apoio da Área de Segurança da Informação, os planos de continuidade de negócios;
- Realizar cópias de segurança (backup restore), garantindo a recuperação de dados essenciais à infraestrutura de tecnologia;
- Garantir a segregação e segmentação de ambiente de rede, para reduzir os riscos de acessos ou modificações acidentais e/ou não autorizadas;
- Executar o controle do antivírus/*antimalware* em todos os servidores, estações de trabalho e notebooks;
- Assegurar o suporte e manutenção da VPN;
- Garantir a proteção do ambiente de todos os ativos críticos de tecnologia da informação;
- Implantar mecanismos de controle de acesso, a fim de garantir a confidencialidade dos dados durante a sua transmissão e armazenamento;
- Revisar periodicamente as autorizações concedidas;
- Aplicar técnicas de criptografia para a proteção da confidencialidade e da integridade das informações críticas, armazenadas ou trafegadas pelos ativos de informação, conforme a Política de Criptografia;
- Garantir a utilização de senhas segura, obedecendo aos requisitos de segurança e complexidade, além do duplo fator de autenticação obrigatório nos acessos às contas dos usuários;
- Monitorar os E-mails dos colaboradores e serviços Microsoft e Azure.

6.5 Compras e Gestão De Fornecedores

Cód. da Política:	Responsável(eis):	Revisão em:	Nº da Revisão:
POL. SIC.001	Segurança da Informação e Cibernética	07/2026	01

- Garantir que terceirizados e fornecedores que manipulam dados originados na NDD Pay assinem os termos de confidencialidade e/ou contrato contendo cláusulas de privacidade, segurança da informação e segurança cibernética, de acordo com a prestação de serviços e atividade, se aplicável.

6.5 Compliance

- Apoiar a Diretoria de Serviços, Infraestrutura e Segurança na elaboração de políticas e procedimentos e na adoção e institucionalização de mecanismos e/ou instrumentos de controle relacionados aos requisitos estabelecidos na presente política;
- Auxiliar a Diretoria de Serviços, Infraestrutura e Segurança na divulgação e nos treinamentos acerca dos requisitos de segurança da Informação e Segurança;
- Ajudar na elaboração e implantação de planos de ação corretivos e preventivos;
- Sugerir adequações das políticas, controles e procedimentos;
- Conduzir processos de verificação de *Compliance*, com a finalidade de checar a eficácia e efetividade dos requisitos estabelecidos na presente política;
- Avaliar, em conjunto com Segurança da Informação e Segurança Cibernética, os riscos inerentes nos ativos de tecnologia da informação da NDD Pay e reportá-los à Diretoria de serviços, Infraestrutura e Segurança;
- Apoiar o Diretor de serviços, Infraestrutura e Segurança, na comunicar, tempestivamente, ao Bacen as ocorrências de incidentes relevantes e interrupções dos serviços relevantes, que configurem situação de crise pela Instituição, bem como das providências para o reinício das suas atividades; e
- Apoiar o Diretor de serviços, Infraestrutura e Segurança, na comunicar ao Bacen das contratações de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem, em até 10 dias úteis da contratação.

6.6 Comitê de Crise

- Avaliar o incidente que ocasionou a interrupção de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem contratados;
- Propor solução(ões) para a crise;
- Envolver todas as partes necessárias e determinar as atribuições de cada uma;
- Decidir sobre o curso de ação.

6.7 DPO (Comitê de Privacidade de Dados Pessoais)

- Tratar os incidentes de segurança da informação que resultarem em violação de Dados Pessoais e/ou Dados Pessoais Sensíveis;
- Recomendar a adoção de medidas remediadoras para mitigar os riscos reputacionais, financeiros e/ou de sanções à Instituição;

Cód. da Política:	Responsável(eis):	Revisão em:	Nº da Revisão:
POL. SIC.001	Segurança da Informação e Cibernética	07/2026	01

- Propor melhorias aos mecanismos ou instrumentos de controle e monitoramento às diretrizes de Privacidade de Dados Pessoais;
- Comunicar à Diretoria da Instituição os incidentes de privacidade que representem risco alto e possam causar impactos negativos relacionados à reputação da organização e gerar externalidades financeiras e/ou que possuam o condão de gerar aplicação de sanções relevantes.

6.8 Gente e Gestão

- Assegurar que todos os ativos fornecidos aos colaboradores, durante a vigência de seu contrato, sejam devolvidos quando ocorrer a extinção do vínculo;
- Informar às áreas responsáveis acerca da remoção de acessos físicos ou acessos lógicos aos sistemas de informação quando ocorrer o desligamento do colaborador ou o encerramento do contrato de prestação de serviço e as alterações de cargo/área.

6.9 Treinamento e Desenvolvimento / Marketing

- Apoiar a Diretoria de Serviços, Infraestrutura e Segurança no treinamento de todos os colaboradores e na conscientização acerca das diretrizes e regulamentos de Segurança da Informação e Segurança Cibernética.

6.8 Gerencias e Lideranças

- Fazer e garantir que seus liderados façam todos os treinamentos necessários, com o intuito de assegurar que as medidas de segurança da informação referentes à sua área estão sendo observadas;
- Avaliar, periodicamente, os privilégios atribuídos a cada Perfil de Acesso.

6.9 Colaboradores /Prestadores de Serviços

- Respeitar as diretrizes de Segurança da Informação e segurança Cibernética estabelecidas nas políticas;
- Fazer todos os treinamentos indicados para o exercício de sua função, e, sempre que sentir necessidade, procurar ajuda/esclarecimentos com a área de Segurança da Informação;
- Conhecer e cumprir os procedimentos de segurança, homologado pela Gerência de Segurança da Informação, com o objetivo de proteger as informações da NDD Pay;
- Notificar a área de Segurança da Informação, sempre que identificar uma violação das diretrizes citadas nesta política;
- Notificar a área de Segurança da Informação caso identifique a existência de fragilidades ou eventos de falha na Segurança Cibernética e Segurança da Informação por meio de e-mail ou grupos no Teams abertos para esses eventos com a gestão imediata, colaborador que identificou o evento, gerente de infraestrutura de segurança da informação;
- Sugerir melhorias de controles, políticas e procedimentos, quando identificar necessidade;

Cód. da Política:	Responsável(eis):	Revisão em:	Nº da Revisão:
POL. SIC.001	Segurança da Informação e Cibernética	07/2026	01

- Assinar, no momento da contratação, o Termo de Aceite ao Código de Compromisso de Confidencialidade e Sigilo.

7 Disposições Gerais

7.1. Vigência e Aprovação

Esta Política tem vigência a partir da data de sua aprovação e divulgação, podendo ser revisada sempre que necessário.

7.2. Consequências e Violações

Qualquer violação à presente política será passível de penalização, que poderá ser desde advertência verbal até demissão por justa causa e, no caso de ocorrência de danos, reparação do eventual dano causado.

As medidas de consequências adotadas pela Instituição, seja no âmbito interno ou por meio de adoção de medida judicial cabível, serão aplicadas após a avaliação da gravidade do caso concreto e dos impactos causados pela violação.

8 Histórico

CONTROLE DE ATUALIZAÇÕES				
Data	Versão	Elaboração	Alteração	Aprovação
01/2026	1.0	Segurança da Informação e Cibernética	Criação do documento	Diretoria
07/2026	2.0	Segurança da Informação e Cibernética	Revisão ampla do documento, inclui atualizações normativas do BACEN + Logo e Nome fantasia	Diretoria

Cód. da Política:	Responsável(eis):	Revisão em:	Nº da Revisão:
POL. SIC.001	Segurança da Informação e Cibernética	07/2026	01

9 ANEXOS

Anexo I - Cartilha de Recomendações e Instruções de Segurança Cibernética para Clientes e Usuários (publicar no site)

1. Proteção de Senhas e Acessos

- Crie senhas fortes, incluindo letras maiúsculas e minúsculas, números e símbolos.
- Nunca compartilhe suas senhas, códigos de segurança (OTP), token ou PIN com terceiros, inclusive com pessoas que afirmem ser da instituição.
- Altere suas senhas regularmente e evite reutilizar a mesma senha em outros serviços.
- Habilite a autenticação de múltiplos fatores (MFA/2FA), sempre que disponível.
- Evite reutilizar senhas em diferentes serviços e realize alterações periódicas.
- Nunca armazene senhas em locais inseguros, como anotações físicas ou arquivos desprotegidos.

2. Cuidados com Dispositivos

- Utilize antivírus e mantenha seu dispositivo atualizado (computador, celular ou tablet).
- Não utilize computadores públicos ou redes Wi-Fi abertas para acessar canais financeiros.
- Ative bloqueio automático de tela em seus dispositivos móveis.
- Não faça download nem instale aplicativos fora das lojas oficiais (Google Play, Apple Store).
- Ative bloqueio automático de tela e utilize biometria ou senha de desbloqueio.

3. E-mails, Links e Golpes

- Cuidado com links recebidos por SMS, *WhatsApp*, redes sociais ou e-mails suspeitos.
- Desconfie de mensagens com ofertas "boas demais", promessa de crédito imediato ou urgência extrema.
- Sempre verifique o domínio do e-mail do remetente (fraudes podem usar endereços parecidos).
- Não compartilhe dados pessoais por chat, redes sociais ou telefone sem verificar a autenticidade do contato.
- Desconfie de mensagens com caráter de urgência, ameaças ou promessas de benefícios financeiros.
- Sempre confira o domínio do remetente (golpistas utilizam endereços semelhantes aos oficiais).
- A NDD Pay não solicita dados pessoais sensíveis por telefone, e-mail ou mensagens, como também nunca irá te pedir seus dados de acesso (login e senha).
- Nunca informe dados pessoais, bancários sem validação do canal oficial.

4. Aplicativos e Sites

- Acesse aplicativos financeiros apenas pelas lojas oficiais e sites digitados diretamente no navegador.
- Confirme se o site possui **cadeado de segurança (https://)** antes de inserir dados.

Cód. da Política:	Responsável(eis):	Revisão em:	Nº da Revisão:
POL. SIC.001	Segurança da Informação e Cibernética	07/2026	01

- Digite o endereço do site diretamente no navegador, evitando acessos por links desconhecidos.
- Nunca salve senhas automaticamente no navegador ao acessar conta ou sistema financeiro.

5. Proteção de Dados Pessoais (LGPD)

- Evite divulgar informações pessoais ou financeiras em redes sociais ou ambientes públicos.
- Não envie fotos de cartões, documentos ou comprovantes por mensageiros sem necessidade.
- Desconfie de solicitações de atualização de cadastro enviadas sem aviso prévio pela instituição.
- Fique atento a ligações solicitando confirmação de dados sensíveis.
- A NDD Pay trata seus dados conforme a Lei Geral de Proteção de Dados (LGPD), utilizando-os apenas para finalidades legítimas e seguras.

6. Segurança em Transações Financeiras (PIX e Pagamentos)

- Confira sempre os dados do recebedor antes de concluir transferências, Pix ou pagamentos.
- Ative limites transacionais no aplicativo e configure limites adicionais para Pix noturno, se disponível.
- Em operações com **cartão de pagamento de frete (IPEF)**, nunca entregue cartão ou senha a terceiros.
- Em caso de dúvida, interrompa a transação e valide a operação antes de prosseguir e se for identificado ser uma transação suspeita, nos comunique imediatamente a instituição.
- A instituição pode realizar **bloqueios preventivos de transações suspeitas**, conforme regulamentação do Banco Central.
- Em caso de fraude ou erro, poderá ser acionado o **Mecanismo Especial de Devolução (MED)** conforme regras do PIX.

7. Golpes Comuns – Alerta

- **Golpe do suporte falso:** alguém liga dizendo ser da instituição para “desbloquear” sua conta.
- **Golpe do QR Code:** nunca aceite QR Code enviado por terceiros sem verificar a origem.
- **Golpe do falso prêmio/ cashback:** cuidado com mensagens prometendo bônus ou benefícios sem origem oficial.
- **Golpe de clonagem do WhatsApp:** não compartilhe códigos de confirmação recebidos por SMS.
- **Clonagem de WhatsApp:** solicitação de códigos recebidos por SMS.
- **Phishing:** páginas falsas que imitam sites oficiais para capturar dados.

8. Monitoramento de Conta

- Ative notificações por SMS, e-mail ou aplicativo para acompanhar movimentações.
- Consulte regularmente seu extrato e comunique imediatamente qualquer atividade estranha.
- Bloqueie temporariamente o cartão ou conta sempre que suspeitar de acesso indevido.
- Mantenha seus dados cadastrais sempre atualizados.

Cód. da Política:	Responsável(eis):	Revisão em:	Nº da Revisão:
POL. SIC.001	Segurança da Informação e Cibernética	07/2026	01

9. Prevenção a fraudes e responsabilidade do usuário

- A segurança das operações depende também do comportamento do usuário.
- O não cumprimento das boas práticas de segurança pode expor o usuário a riscos de fraude.
- A NDD Pay monitora continuamente transações e poderá solicitar validações adicionais para garantir a segurança.

10. Canal de Ajuda

Se você identificar qualquer suspeita de fraude, acesso indevido ou transação irregular:

- Contate imediatamente o canal oficial da Instituição.
- Solicite o bloqueio de acesso ou transações, se necessário.
- Bloqueie acesso via aplicativo ou central, se disponível.
- registre boletim de ocorrência, se necessário.

Em caso de dúvidas, suspeitas ou incidentes de segurança, utilize exclusivamente os canais oficiais da NDD Pay disponibilizados no site institucional.