OUTUBRO 2025

Netz asset

Política de Segurança da Informação

SUMÁRIO

1. INTRODUÇÃO E OBJETIVO

Esta Política de Segurança da Informação ("Política") estabelece os princípios, regras e conceitos básicos que nortearão a Netz Asset ("Netz", "Netz Asset"ou "Asset") em sua atuação no âmbito da Área de Tecnologia e Segurança da Informação.

Cumpre salientar que a Netz Asset faz parte da Netz Holding, que é um Grupo Econômico que exerce diversas atividades, visando sempre um atendimento personalizado, de qualidade e integridade para todos os seus clientes. Os serviços atualmente prestados são os de: (i) Consultoria[1]; (ii) Câmbio, Seguros e Banking[2]; (iii) Securitizadora[3]; e (iv) Gestão de Fundos de Investimentos e Gestão de Patrimônio[4]. Todas as atividades observam as normas regulatórias e autorregulatórias, melhores práticas do mercado, mitigando conflitos de interesse e prestando de um serviço de excelência e alto impacto.

O propósito da Netz Holding é cuidar do patrimônio para que pessoas extraordinárias possam dedicar sua energia ao que realmente importa.

Este documento tem a finalidade de descrever as principais regras, princípios, diretrizes e escopo de atuação das Áreas de Tecnologia e Segurança da Informação e Infraestrutura da Netz Asset, incluindo:

- Segurança da Informação;
- Aquisição e instalação de hardware e software;
- Contratação de serviços;
- Serviços de Help Desk;
- Inventário de bens de informação;
- Controle de acessos;
- Segurança de hardware e software;
- Comunicação de dados e voz;
- Plano de Contingência;
- Uso dos recursos de informação.

2. BASE LEGAL

(i) Resolução da Comissão de Valores Mobiliários ("CVM") n° 21, de 25 de fevereiro de 2021 ("Resolução CVM 21");

(ii) Regras e Procedimentos de Deveres Básicos Anbima ("RP Deveres Básicos Anbima");

---

[1] Netz Solutions LTDA, CNPJ n°60.408.897/0001-19
[2] Netz Select Corretora de Seguros LTDA., CNPJ n° 39.151.020/0001-07 e Netz Corretora de Seguros LTDA., CNPJ n° 61.734.108/0001-00
[3] Netz Securitizadora de Créditos, CNPJ n° 61.833.005/0001-90
[4] Netz Asset Gestão de Recursos LTDA., CNPJ n° 48.638.617/0001-63

(iii) Guia Anbima de Orientações para Contratação de Terceiros e Nuvem (“Guia Anbima”);
(iv) Modelo de Política de Desenvolvimento Seguro de Aplicações da Anbima (*Softwares*);
(v) Lei nº 13.709 de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (“LGPD”); e
(vi) Demais manifestações e ofícios orientadores dos órgãos reguladores e autorregulados aplicáveis.

3. PRINCÍPIOS E DIRETRIZES DE SEGURANÇA DA INFORMAÇÃO

A Segurança da Informação na Netz Asset baseia-se nos seguintes princípios fundamentais:

- Confidencialidade: garantia de que a informação é acessível apenas a pessoas autorizadas;
- Integridade: manutenção da exatidão e consistência das informações;
- Disponibilidade: garantia de acesso a informação sempre que necessário para a execução das atividades corporativas;
- Autenticidade e Rastreabilidade: verificação da identidade de usuários e rastreamento das ações realizadas nos sistemas;
- Legalidade e Conformidade: aderência às normas legais, regulatórias e autorregulatórias; e
- Proporcionalidade: adoção de medidas de segurança compatíveis com o porte da Netz Asset, grau de risco e criticidade do dos dados e informações.

A Netz compromete-se a proteger suas informações contra perda, acesso não autorizado, divulgação indevida, destruição acidental ou uso inadequado, promovendo uma cultura de segurança, confidencialidade e responsabilidade digital.

4. GOVERNANÇA E RESPONSABILIDADE

A gestão da Tecnologia e Segurança da Informação é uma atribuição estratégica da Diretoria de Governança, Risco e Compliance (GRC) em conjunto com a Área de Tecnologia da Informação, contando com a colaboração, sempre que necessário, de outras áreas da Netz, incluindo, mas não se limitando à Área de Infraestrutura.

Além da Área de Tecnologia da Informação, a Asset possui uma Área de Infraestrutura, que é responsável pela instalação, manutenção e suporte técnico de equipamentos e dispositivos eletrônicos, bem como pela gestão da rede física, cabeamento estruturado, conectividade e controle ambiental das instalações.

4.1. Diretoria de Governança, Risco e Compliance (GRC)

Compete à Diretoria de GRC:

- Coordenar e revisar esta Política e suas atualizações;
- Supervisionar o cumprimento de todas as previsões contidas nesta Política, das normas de segurança e privacidade;
- Coordenar e determinar acessos de usuários nos sistemas internos e externos;
- Apoiar a implementação de controles internos de proteção da informação;
- Garantir a aderência às normas legais, regulatórias e autorregulatórias;
- Avaliar incidentes de segurança e determinar as medidas corretivas através de Planos de Ação estruturados; e
- Manter registros e evidências dos controles aplicados.

4.2. Área de Tecnologia da Informação (TI)

Compete à Área de TI:

- Implementar e manter controles técnicos e operacionais de proteção da informação;
- Gerenciar acessos, senhas e permissões de usuários nos sistemas internos em conjunto com a Área de GRC;
- Realizar cópias de segurança (backups) e testes periódicos de restauração em conjunto com a Área de GRC e Área de Infraestrutura;
- Garantir a disponibilidade e resiliência dos sistemas e redes corporativas em conjunto com a Área de Infraestrutura;
- Desenvolver sistemas internos para aprimoramento das atividades da Netz Asset, garantindo segurança, viabilidade e qualidade dos serviços e informações; e
- Apoiar o tratamento de incidentes e vulnerabilidades.

4.3. Área de Infraestrutura

Compete à Área de Infraestrutura:

- Garantir o pleno funcionamento dos aparelhos, servidores locais e dispositivos de comunicação;
- Realizar manutenção preventiva e corretiva de hardware e equipamentos de rede;
- Gerenciar acessos, senhas e permissões de usuários nos sistemas em conjunto com a Área de GRC;

- Atuar nas atividades de instalação, substituição e inventário de ativos tecnológicos em conjunto com a Área de TI, quando necessário;
- Assegurar redundância elétrica e conectividade contínua;
- Zelar pela segurança física dos equipamentos e controle de acesso a ambientes técnicos.

4.4. Colaboradores e Terceiros

Todos os colaboradores[5] e terceiros com acesso às informações da Netz Asset devem:

- Cumprir as diretrizes desta Política e dos demais documentos internos[6];
- Manter suas senhas de acesso e sistema de autentificação de dois fatores protegidas, sem compartilhamento entre áreas e/ou colaboradores[7];
- Proteger as informações contra acesso ou divulgação não autorizada;
- Atuar com diligência e zelo quando sua atividade envolver dados pessoais e/ou outras informações confidenciais;
- Utilizar os sistemas e equipamentos corporativos para o regular desempenho de suas atividades profissionais; e
- Reportar imediatamente à GRC qualquer incidente, falha ou suspeita de violação de segurança.

5. GESTÃO DE ACESSOS E IDENTIDADES

A gestão de acessos visa garantir que somente usuários devidamente autorizados tenham acesso a determinadas informações e sistemas, de acordo com o cargo e a atividade exercida na Netz.

5.1. Controle de Acessos

- Os acessos aos sistemas internos e externos serão liberados de acordo com o cargo e área em que o colaborador exerce sua função e devem ser devidamente registrados pela Área de Tecnologia da Informação ou Infraestrutura, e, deverão ser aprovados pela Diretoria de GRC, quando necessário;
- Cada colaborador possui um usuário individual e intransferível, com senha pessoal e expiração periódica;

[5] Tal como definido no Código de Ética da Netz Holding.
[6] Especialmente, mas não somente nas regras previstas no item 5 do Código de Ética.
[7] É utilizado o aplicativo Authenticator (MFA) da Microsoft.

- O acesso será concedido de acordo com a necessidade da sua função e da área, mitigando o acesso a informações que não sejam necessárias à sua atividade;
- Contas inativas ou de colaboradores desligados devem ser bloqueadas imediatamente; e
- O compartilhamento de senhas ou dispositivos de autenticação é vedado.

5.2. Monitoramento e Auditoria

Todos os arquivos e registros de acesso deverão ser mantidos pelo prazo mínimo de 05 anos.

Quando houver qualquer suspeita ou incidente de acesso indevido em sistemas e/ou informações, a Diretoria de GRC deverá ser formalmente notificada para que sejam avaliados os riscos, impactos e eventuais procedimentos necessários, além da criação de Plano de Ação formal para que os impactos sejam os menores possíveis e para mitigar qualquer incidente similar.

Caberá à Diretoria de GRC a auditoria interna e monitoramento periódico para verificar os acessos, disponibilidade, manutenção e arquivamento das informações.

6. AQUISIÇÃO, INSTALAÇÃO E MANUTENÇÃO DE SERVIÇOS DE TI

A aquisição de qualquer software e/ou sistema observará as diretrizes de segurança e integridade da informação, do Guia Anbima, além de ser submetido a due diligence pela Área de GRC, que deverá, inclusive, aprovar a contratação. Após as análises, as Áreas de Infraestrutura e TI homologarão o sistema antes da instalação e utilização.

Qualquer sistema, extensão ou programa não homologado não poderá ser utilizado.

Todos os equipamentos serão protegidos por antivírus, firewall e mecanismos de detecção de invasão e sua manutenção só poderá ser feita pela Área de Infraestrutura.

Qualquer serviço ou sistema que for responsável pelo tratamento, armazenamento, hospedagem ou acesso a informações da Netz só poderá ser contratado após as avaliações supracitadas, além da análise prévia de risco

para identificação da segurança da informação, continuidade, tratamento, exclusão e/ou anonimização dos dados e confidencialidade[8].

Quando houver necessidade de acesso a sistemas corporativos por terceiros, este ocorrerá sob supervisão e com rastreamento específico.

A análise da prestação de serviços deverá ser feita em conjunto pelas Áreas de TI e Infraestrutura com reporte à Área de GRC, que será responsável pela comunicação e tratamento de eventuais incidentes e/ou erros operacionais.

7. PROTEÇÃO CONTRA AMEAÇAS CIBERNÉTICAS E MALWARE

A Netz Asset adota medidas preventivas e corretivas para reduzir o risco de incidentes cibernéticos e contaminações por malware. Assim, todos os equipamentos e sistemas estão protegidos por antivírus, firewall e antimalware.

Periodicamente os dispositivos e servidores são atualizados para manutenção das proteções, além de estar proibido o uso de mídias externas (tal como pendrives e HDs externos)[9]. Com o intuito de mitigar ameaças, também é proibida a instalação de softwares não autorizados.

Qualquer suspeita de ameaça deverá ser reportada as Áreas de TI e Infraestrutura que envolverão a Área de GRC para apuração e coordenação de resposta a qualquer incidente.

8. CÓPIAS DE SEGURANÇA E CONTINUIDADE DOS NEGÓCIOS

A Netz Asset mantém procedimentos formais de backup, recuperação e continuidade operacional, assegurando a integridade e a disponibilidade das informações em situações de falha ou contingência.

Os arquivos são armazenados em nuvem e o backup é feito em tempo real, assim, caso haja qualquer incidente e/ou ocorrência que impeça os colaboradores de estarem presencialmente no escritório, os arquivos e sistemas poderão ser acessados remotamente. O backup em tempo real também é uma forma de validar e verificar os sistemas diariamente.

Ainda assim, a Netz realiza um teste anual de continuidade dos negócios[10] que é coordenado pela Diretora de GRC com apoio das Áreas de TI e Infraestrutura.

---

[8] Os contratos firmados deverão possuir cláusulas específicas sobre a proteção de dados e sigilo, de acordo com a LGPD e as previsões dos órgãos regulatórios e autorregulatórios.
[9] Se houver necessidade, a liberação só poderá ocorrer após a autorização da Diretora de GRC.
[10] Tal como previsto no Plano de Continuidade de Negócios.

O teste é devidamente documentado e armazenado para monitoramento e acompanhamento.

9. USO DE E-MAIL, INTERNET E EQUIPAMENTOS CORPORATIVOS

Os recursos tecnológicos da Netz Asset são de uso exclusivamente profissional e devem ser utilizados com responsabilidade e ética, tal como previsto no Código de Ética. Assim:

- É proibido o uso de e-mail corporativo para fins pessoais, divulgação de informações confidenciais ou envio de conteúdo inapropriado;
- O acesso à internet deve restringir-se a sites e serviços relacionados às atividades profissionais;
- É vedada a utilização de plataformas de armazenamento em nuvem não corporativas, quando há necessidade de compartilhamento de arquivos com terceiros, deve ser solicitada a liberação à Área de Infraestrutura;
- O compartilhamento de arquivos e informações sensíveis deve ocorrer apenas por canais homologados e já utilizados internamente; e
- As Áreas de TI e Infraestrutura poderão monitorar logs e tráfego de rede para garantir o cumprimento desta Política, respeitando os limites legais e de privacidade previstos na LGPD.

A Área de Infraestrutura é responsável pelo inventário dos equipamentos utilizados pelos colaboradores da Netz.

10. TREINAMENTO

Todos os colaboradores devem participar de programas periódicos de conscientização e capacitação em segurança da informação e proteção de dados, coordenados pela Diretora de GRC, que abordarão, dentre outros temas:

- Boas práticas de segurança digital e uso responsável da informação;
- Prevenção a ataques cibernéticos e engenharia social;
- Procedimentos de reporte de incidentes;
- Obrigações legais e regulatórias; e
- Condutas éticas e responsabilidade individual.

11. HELP DESK

Nos casos de necessidade de recurso adicional e/ou necessidade de suporte, o colaborador deverá fazer a solicitação para a Área de Infraestrutura através do sistema interno de Help Desk.

A depender do tipo de solicitação, o responsável pela área deverá autorizar a liberação. O sistema é passível de auditoria e é possível acompanhar o número de solicitações feitas, prazo de atendimento, dentre outros.

12. VIGÊNCIA E ATUALIZAÇÃO

Histórico das atualizações		
Data	Versão	Tópicos
Janeiro/2025	1ª	Constituição da Netz
Outubro/2025	2ª	Atualização – Netz Holding e práticas