Política de Segurança Cibernética

1. Introdução

Esta Política aborda as diretrizes, atribuições e responsabilidades no processo de Segurança Cibernética às instituições integrantes do conglomerado das empresas Bitso do Brasil, quais sejam: Nvio Brasil Instituição de Pagamento Ltda. (líder do conglomerado prudencial) e Nvio Brasil Sociedade de Crédito Direto S.A. (conjuntamente denominadas simplesmente como "Companhia" ou "Bitso do Brasil"), devendo ser seguida por todos os seus Colaboradores e Parceiros de Negócios.

2. Objetivo

Estabelecer as diretrizes para compor um programa de Segurança Cibernética na Companhia.

3. Abrangência

Esta Política abrange todas as ferramentas, aplicações, processos e monitoramento de Segurança da Informação e Segurança Cibernética no ambiente da Companhia, independente da sua localização física.

4. Definições

- “Contrato” significa o Contrato Social
- “Diretoria” significa a Diretoria da Companhia.
- “Bacen” significa o Banco Central do Brasil
- “CISO” significa o Diretor de Segurança da Informação
- “CMN” significa o Conselho Monetário Nacional
- "Companhia" significa Grupo Bitso Brasil.
- “CTO” significa o Diretor de Tecnologia
- “Diretores” significa o Diretor ou os Diretores pessoa física na Diretoria da Companhia
- "Política” significa a Política de Governança Corporativa
- “Resolução 4.893” significa a Resolução nº 4.893, de 26 de fevereiro de 2021, aprovada pelo Conselho Monetário Nacional.

5. Atribuições e Responsabilidades

A Companhia designará um executivo de nível sênior dentro da organização responsável por estabelecer e manter uma estratégia adequada de segurança da informação e gestão de incidentes orientando o pessoal na identificação, implementação e manutenção dos controles que auxiliam a

garantir a disponibilidade, integridade e disponibilidade dos ativos de informações da Companhia. Este profissional será denominado como Chief Information Security Officer, doravante CISO.

As principais responsabilidades do CISO incluem, mas não estão limitadas a:

- Verificar e ser responsável pela implementação e conformidade contínua com as políticas de segurança da informação e procedimentos dentro da organização.
- Elaborar um plano estratégico de segurança que contém os projetos a serem realizados anualmente, com o objetivo de fortalecer a segurança das informações da Companhia.
- Revisar e ser responsável pela aprovação de políticas que orientem o sistema de gestão de segurança da informação da Companhia.
- Validar, pelo menos anualmente, a necessidade dos negócios para acessar a infraestrutura tecnológica, de acordo com os perfis de trabalho (segregação funcional), inclusive aqueles com privilégios altos, como administração dos sistemas, bancos de dados e aplicativos operacionais.
- Gerenciar os incidentes de segurança, considerando os estágios de detecção, contenção, erradicação, recuperação e notificação.
- Presidir a equipe encarregada de detectar e responder aos incidentes de segurança, bem como ser responsável por manter um canal de comunicação com o Comitê de Risco, a fim de informar sobre os incidentes detectados e as providências a serem tomadas.
- Verificar a implementação correta dos programas anuais de treinamento destinados a todo o pessoal da Companhia, bem como conhecimento de segurança da informação para clientes, inclusive, se for o caso, terceiros que prestam serviços a eles.
- Apresentar relatórios de segurança da informação e projetos para o CEO e para as diretorias e comitês necessários.
- Gerar, avaliar e manter indicadores de risco de segurança da informação e informar os resultados para a área de Risco Corporativo.
- Garantir a conformidade com os regulamentos aplicáveis, atendendo, de forma apropriada e oportuna, às exigências estabelecidas pelas autoridades
- Gerar e implementar planos de melhorias contínuas em termos de segurança da informação, que devem estar alinhados com os objetivos comerciais da Companhia.
- Participação em auditorias internas e externas.
- Elaborar o Relatório Anual.

Todos os colaboradores e prestadores de serviço da Companhia devem estar plenamente comprometidos com a segurança cibernética em todos os níveis de serviço, sendo responsáveis por:

- Ler atentamente esta Política, declarar ciência e aderir às diretrizes que constam neste documento;
- Tratar as informações de uma maneira ética e confidencial, de acordo com as políticas e procedimentos atuais sobre segurança da informação da Companhia;

- Assegurar ininterruptamente a proteção das informações da Companhia contra o acesso, a modificação, destruição ou divulgação não autorizada;
- Notificar quaisquer incidentes, pontos fracos ou quebras de segurança para as equipes de Segurança da Informação e de Risco;
- Participar dos treinamentos e conscientização sobre práticas de Segurança da Informação que venham a ser oferecidos pela Companhia;
- Colaborar com a área de Segurança da Informação no monitoramento e supervisão de suas atividades profissionais, sejam estas realizadas em ambientes físicos ou eletrônicos (incluindo notebooks, e-mails, telefones corporativos, pendrives, entre outros), independentemente de aviso prévio, estando ciente tratar-se de ferramentas de trabalho e, portanto, não podendo alegar invasão de privacidade;
- Reconhecer e aceitar que, no caso de violação a qualquer diretriz ou procedimento aqui previstos, estará sujeito, além das medidas disciplinares aplicáveis, à responsabilização por eventuais danos causados, nos termos da legislação aplicável.

6. Diretrizes

Os incidentes de segurança da informação podem ser notificados por qualquer usuário da Companhia ou identificados por áreas da Tecnologia da Informação “TI”.

7. Plano de Segurança Cibernética

- Proteger as informações contra acesso, modificações, destruição ou divulgação não autorizada.
- Prover a adequada classificação da informação, sob os critérios de confidencialidade, disponibilidade e integridade.
- Assegurar que os recursos utilizados para o desempenho de sua função sejam utilizados apenas para as finalidades aprovadas pela Companhia.
- Garantir que os sistemas e as informações sob responsabilidade da Companhia estejam adequadamente protegidos.
- Garantir a continuidade do processamento das informações críticas de negócios.
- Selecionar os mecanismos de segurança da informação, balanceando fatores de riscos, tecnologia e custo.
- Comunicar imediatamente à área de Segurança da Informação, quaisquer descumprimentos da Política Corporativa de Segurança da Informação.

8. Proteção do Ambiente

Devem ser constituídos controles e responsabilidades pela gestão e operação dos recursos de processamento das informações que garantem a segurança na infraestrutura tecnológica de redes

locais e internet, através de um gerenciamento efetivo no monitoramento, tratamento e respostas aos incidentes, para minimizar o risco de falhas e a administração segura de redes de comunicações, incluindo a gestão de serviços contratados de processamento e armazenamento de dados e informações em nuvem.

9. Segurança Física e Lógica

Os equipamentos e instalações de processamento de informação críticas ou sensíveis devem ser mantidos em áreas seguras, com níveis e controles de acesso apropriados, incluindo proteção contra ameaças físicas e ambientais.

Os requisitos de segurança de sistemas de informação devem ser identificados e acordados antes do seu desenvolvimento e/ou de sua implementação, para que assim possam ser protegidos visando a manutenção de sua confidencialidade, integridade e disponibilidade.

Os colaboradores, prestadores de serviço e terceiros da Companhia devem ser treinados periodicamente sobre os conceitos de Segurança da Informação, através de um programa de conscientização.

10. Gestão de Acesso

O controle de acesso aos nossos ativos de informações é uma parte fundamental de uma estratégia de defesa em profundidade da segurança da informação. A Companhia estabelece exigências específicas para proteger os ativos de informações contra o acesso não autorizado.

11. Processamento, Armazenamento de Dados e Computação em Nuvem (Cloud)

Conforme a Resolução 4.893/2021 do Banco Central do Brasil, para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem, a Companhia deve possuir procedimentos efetivos para a aderência às regras previstas na regulamentação em vigor.

12. Continuidade de Negócios

O processo de gestão de continuidade de negócios relativo a segurança da informação deve estar em permanente funcionamento para minimizar os impactos e recuperar perdas de ativos da informação, após um incidente crítico, a um nível aceitável, através da combinação de requisitos como operações, funcionários chaves, mapeamento de processos críticos, análise de impacto nos negócios e testes periódicos de recuperação de desastres. Incluem-se nesse processo, a continuidade de negócios

relativos aos serviços contratados de nuvem e os testes previstos para os cenários de ataques cibernéticos.

13. Treinamento e Conscientização

Um programa de conscientização em Segurança Cibernética à garantia dos objetivos e diretrizes definidos nesta Política é realizado adequando-se às necessidades e responsabilidades específicas de cada colaborador e, onde pertinente, terceiros da Companhia.

14. Resposta a Incidentes de Segurança da Informação

O procedimento estabelecido nesta seção deverá ser usado somente como orientação ao responder a um incidente. A natureza exata de um incidente e seu impacto não podem ser previstos com qualquer grau de certeza e é tão importante que um bom grau de senso comum seja usado ao decidir as medidas a serem tomadas.

15. Vigência

Esta Política entra em vigor na data indicada no quadro do cabeçalho e deverá ser revisada: (i) obrigatoriamente a cada 1 ano; (ii) em caso de alteração na legislação aplicável que impacte o disposto nesta PO; (iii) quando houver determinação expressa nesse sentido por parte dos órgãos reguladores; (iv) quando houver alteração dos processos internos da Companhia que altere as diretrizes aqui descritas.

16. Registro de Alterações

Versão nº	Data de Elaboração	Elaborador	Data de Revisão	Revisor	Descrição de Mudanças
1.0	Outubro/2022	Cibersegurança	Março/2023	Compliance	Versão inicial
1.1	Março/2024	Cibersegurança	Março/2024	Compliance	Revisão anual e textual