Política de Segurança da Informação e Segurança Cibernética

Dezembro de 2023 – Versão 3

FICHA DE CONTROLE

Informações Gerais

Título	Política de Segurança da Informação e Segurança Cibernética
Número da Versão	V.03
Status	Aprovada
Aprovador	Diretoria
Data da aprovação	18.12.2023
Data da próxima revisão	18.12.2024
Procedimentos e outrosdocumentos associados	Lei nº 13.709/18 (LGPD) Resolução nº 4.893/2021 do Conselho Monetário Nacional Resolução 4.557/2017 do Conselho Monetário Nacional Resolução 4.606/2017 do Conselho Monetário Nacional
Normas internas	
Histórico de Versões	V.01 – 30.06.2018 V.02 – 15.12.2020 V.03 – 31.10.2023

OBJETIVO

A Política de Segurança da Informação e Segurança Cibernética (“Política”) tem por escopo estabelecer os princípios, diretrizes e atribuições relacionadas à segurança da informação, protegendo as informações da VIPe, dos seus clientes e do público em geral, observando as melhores práticas de mercado e regulamentações aplicáveis.

PÚBLICO-ALVO

Colaboradores da VIPE.

ALÇADA DE APROVAÇÃO

Nos termos do artigo 9º, da Resolução n.º 4.893/2021, esta Política foi devidamente aprovada e será revisada seguindo a metodologia apresentada abaixo:

- Diretoria: Responsável pela aprovação desta Política e suas respectivas atualizações.
- Auditoria Interna: Responsável pela avaliação anual desta Política.
- Departamento de Tecnologia da Informação: Responsável pela elaboração, aprovação e revisão anual desta Política.
- Departamento de Compliance: Corresponsável pela revisão anual desta Política.

DISPONIBILIZAÇÃO DA POLÍTICA

A presente Política estará disponível no seguinte endereço eletrônico: https://vipe.clickcompliance.com/, e será ficara disponível a todos os colaboradores, da VIPE no mesmo lugar *(ClickCompliance)*. Ainda, esta Política será objeto de reuniões e

treinamentos virtuais ou presenciais, registrados pelo Departamento de Tecnologia da Informação.

INTRODUÇÃO

A informação é um dos principais bens da instituição. Assim, a VIPE define a estratégia de segurança da Informação e segurança cibernética para proteger a integridade, disponibilidade e confidencialidade da informação.

Esta estratégia é baseada na detecção, prevenção, monitoramento e resposta à incidentes e fortalece a gestão do risco de segurança cibernética e a construção de um alicerce robusto para o futuro cada vez mais digital da VIPE.

Para alcançarmos esse objetivo, utilizamos a estratégia de proteção de perímetro expandido. Esse conceito considera que a informação deve ser protegida independentemente de onde esteja, seja internamente, em uma coligada, em um correspondente bancário, em todo o seu ciclo de vida, desde a coleta até o descarte.

PRINCÍPIOS DE SEGURANÇA DA INFORMAÇÃO

Nosso compromisso com o tratamento adequado das informações da VIPE, clientes e público em geral está fundamentado nos seguintes princípios:

- Confidencialidade: garantir que o acesso à informação seja obtido somente por pessoas autorizadas;
- Disponibilidade: garantir que as pessoas autorizadas tenham acesso à informação sempre que necessário;
- Integridade: garantir a exatidão e a completude da informação e dos métodos de seu processamento, bem como da transparência no trato com os públicos envolvidos.

DIRETRIZES

Esta Política deverá ser cumprida integralmente por todos os colaboradores da VIPE, sendo que eventuais ações ou procedimentos que configurem exceções as suas diretrizes somente poderão ser efetivados mediante a autorização da Gerência de Tecnologia da Informação, a qual deverá registrar, reportar e, se for o caso, publicar tais exceções.

A adesão à essa Política e eventuais desvios são reportados periodicamente pela área de Segurança da Informação e Segurança Cibernética ao Comitê Executivo, Comitê de Auditoria e Departamento de Compliance.

A informação deve ser utilizada de forma transparente, para as finalidades informadas ao cliente e de acordo com a legislação vigente. As diretrizes e eventuais exceções são complementadas em procedimentos com regras específicas que devem ser observadas.

PROCESSOS DE SEGURANÇA DA INFORMAÇÃO

Para assegurar que as informações tratadas estejam adequadamente protegidas, a VIPe adota os seguintes processos:

a) Gestão de Ativos

Entende-se por ativo, tudo aquilo que a instituição considerar como relevante para o negócio, desde ativos tecnológicos (p.ex. software e hardware) como não tecnológicos (p.ex. pessoas, processos e dependências físicas) desde que estejam relacionados à proteção da informação.

Os ativos, de acordo com sua criticidade, devem ser identificados, inventariados, mantidos atualizados, possuir um proprietário e ser protegidos contra acessos indevidos. A proteção pode ser física (p.ex. salas com acesso controlado) e lógica (p.ex. configurações de blindagem ou hardening, patch management, autenticação e autorização). Os ativos da VIPE Financeira, dos clientes e do público em geral devem ser tratados de forma ética e sigilosa e de acordo com as leis vigentes e normas internas,

promovendo o uso adequado e prevenindo exposição indevida das informações.

b) Classificação da Informação

As informações devem ser classificadas de acordo com a confidencialidade, conforme Critérios para Classificação e Gestão da Informação para o Brasil, definidos em política interna e Diretrizes de Segurança da Informação, também definidos em política interna. Para isso, devem ser consideradas as necessidades relacionadas ao negócio, o compartilhamento ou restrição de acesso e os impactos no caso de utilização indevida das informações. De acordo com a classificação da confidencialidade, devem ser estabelecidas as proteções necessárias durante todo o seu ciclo de vida. O ciclo de vida da informação compreende: Geração, Manuseio, Armazenamento, Transporte e Descarte.

c) Gestão de Acessos

As concessões, revisões e exclusões de acesso devem utilizar as ferramentas e os processos corporativos da VIPE.

Os acessos devem ser rastreáveis, a fim de permitir a identificação individual do colaborador ou prestador de serviço que tenha acessado ou alterado as informações, permitindo sua responsabilização.

A concessão de acessos deve obedecer ao critério de menor privilégio, no qual os usuários devem ter acesso somente aos recursos de informação imprescindíveis para o pleno desempenho de suas atividades e que sejam devidamente autorizados.

A segregação de funções deve permear todos os processos críticos, evitando que um único responsável possa executar e controlar o processo durante todo seu ciclo de vida. A identificação de qualquer colaborador deve ser única, pessoal e intransferível, qualificando-o como responsável pelas ações realizadas.

A senha é uma informação confidencial, pessoal e intransferível, sendo proibido seu compartilhamento.

d) Gestão de Riscos

Os riscos devem ser identificados por meio de um processo estabelecido para análise de ameaças, vulnerabilidades, probabilidades e impactos sobre os ativos da VIPE, para que sejam recomendadas as proteções adequadas. As recomendações são discutidas nos fóruns apropriados.

Produtos, processos e tecnologias devem ter a adequada gestão dos riscos de Segurança da Informação, para redução dos riscos à níveis aceitáveis, independentemente de estarem dentro da infraestrutura da VIPE, parceiros ou prestadores de serviços.

As tecnologias em uso pela instituição devem estar em versões suportadas pelos seus fabricantes e devidamente atualizadas. Eventuais exceções devem ser aprovadas na alçada competente ou possuir controles compensatórios.

e) Gestão de Riscos em Prestadores de Serviços

Os prestadores de serviços contratados pelo Instituição devem ser classificados considerando alguns critérios, conforme descrito no anexo de Avaliação de Riscos em Segurança da Informação de Fornecedores do documento de Avaliação de Riscos em Segurança da Informação.

Dependendo da classificação, o prestador de serviços passará por avaliação de risco, que pode incluir a validação in loco dos controles de Segurança da Informação, avaliação remota das evidências ou outras avaliações, além do acompanhamento de eventuais correções e melhorias implementadas pelos prestadores de serviços.

Os prestadores de serviços devem informar os incidentes relevantes, relacionados às informações da VIPE armazenadas ou processadas por eles em cumprimento às determinações legais e regulamentares.

f) Tratamento de Incidentes de Segurança da Informação e Segurança Cibernética

A área de Segurança da Informação e Segurança Cibernética, por meio de seu parceiro externo, monitora a segurança do ambiente tecnológico da VIPE, analisando os eventos e alertas para identificar possíveis incidentes.

Os incidentes que são identificados pelos alertas são classificados com relação ao impacto, de acordo com os critérios adotados pela VIPE. Para o seu grau de relevância, serão considerados aspectos como comprometimento de dados de clientes e impacto ao sistema financeiro. Incidentes classificados como relevantes devem ser comunicados ao Regulador.

Todos os incidentes passam por um processo de tratamento e comunicação, onde são registradas todas as informações pertinentes aos incidentes como causa, impacto, classificação, dentre outros.

Informações sobre incidentes que possam impactar outras instituições financeiras devem ser compartilhadas com as demais instituições, visando colaborar com a mitigação do risco conforme determinações legais e regulamentares.

A área de Segurança da Informação e Segurança Cibernética elaborará um Relatório Anual contendo os incidentes relevantes ocorridos no período, ações realizadas de prevenção e resposta aos incidentes e resultados dos testes de continuidade de acordo com as melhores práticas determinadas pelo Itil e Cobit. Este relatório deverá ser apresentado ao Comitê de Risco e à Diretoria, conforme determinações legais e regulamentares.

Visando aprimorar a capacidade de resposta a incidentes, a VIPE realizará testes de continuidade de negócios, simulando cenários de incidentes críticos de Segurança Cibernética, que podem comprometer a disponibilidade e/ou a confidencialidade das informações.

Todo colaborador deve ser proativo e diligente na identificação, comunicação para a área de Segurança da Informação e na mitigação dos riscos relacionados à segurança da informação.

g) Conscientização e Treinamentos em Segurança da Informação e Segurança Cibernética

A VIPE promove a disseminação dos princípios e diretrizes de Segurança da Informação e Segurança Cibernética por meio de programas de conscientização e capacitação para fortalecer a cultura de segurança da informação e cibernética.

Ao menos anualmente, são disponibilizadas campanhas de conscientização ou treinamentos que podem ser presenciais ou on-line, relacionados a confidencialidade, integridade e disponibilidade da informação. Estas campanhas são veiculadas através de e-mails, portal corporativo, e-learning, ou redes sociais aos colaboradores e clientes.

h) Governança com as Áreas de Negócios

As iniciativas e projetos das áreas de negócios devem estar alinhadas com os princípios e diretrizes de segurança da informação e segurança cibernética.

i) Segurança Física do Ambiente

O processo de Segurança Física estabelece controles relacionados à concessão de acesso físico aos ambientes, de acordo com a criticidade das informações tratadas nestes ambientes.

j) Segurança no Desenvolvimento de Sistemas de Aplicação

O processo de desenvolvimento de sistemas deve garantir a aderência aos documentos Desenvolvimento Seguro para o Brasil e boas práticas de segurança da instituição.

Os ambientes produtivos devem ser segregados dos demais ambientes e com acesso somente via aplicação por usuários previamente autorizados ou por ferramentas homologadas.

k) Gravação de Logs

É obrigatória a gravação de logs ou trilhas de auditoria do ambiente computacional, para todas as plataformas, de forma a permitir identificar: quem fez o acesso, quando o acesso foi feito, o que foi acessado e como foi acessado. Essas informações devem ser protegidas contra modificações e acessos não autorizados.

l) Programa de Segurança Cibernética

O Programa de Segurança da Informação e Segurança Cibernética da VIPE é norteado pelos seguintes fatores:

- Regulamentações vigentes;
- Melhores práticas;
- Cenários mundiais;
- Análises de risco da própria instituição.

Conforme sua criticidade, as ações do programa dividem-se em:

- Críticas: Consiste em correções emergenciais e imediatas para mitigar riscos iminentes;
- Sustentação: Iniciativas de curto/médio prazo, para mitigação de risco no ambiente atual, mantendo o ambiente seguro, respeitando o apetite de risco da instituição e permitindo que ações de longo prazo/estruturantes possam ser realizadas;
- Estruturantes: Iniciativas de médio/longo prazo que tratam a causa raiz dos riscos e que preparam o banco para o futuro.

m) Proteção de perímetro

Para proteção da infraestrutura da VIPE contra um ataque externo, utilizamos, no mínimo, ferramentas e controles contra: ataques de DDoS,

Spam, Phishing, APT/Malware, Firewalls de borda, WAF, AKS, invasão de dispositivos de rede e servidores, ataques a aplicação e scan externos.

Para mitigação do risco de vazamento de informações utilizamos ferramentas preventivas instaladas em dispositivos móveis, estações de trabalho, no serviço de correio eletrônico, no serviço de navegação WEB, no serviço de impressão, além do uso de criptografia para dados em repouso e em transporte.

Visando elevar a proteção, não é permitida a conexão física ou lógica à rede corporativa da instituição, por equipamentos particulares ou não homologados.

n) Governança de TI

O Departamento de Tecnologia da Informação abrange as seguintes áreas e comitês relacionados a esta Política: a) área de Segurança da Informação e Segurança Cibernética; b) Comitê de Segurança Corporativa (Governança de TI); e c) Comitê de Auditoria em Segurança da Informação. Tal área e comitês se reportam à Gerência de Tecnologia da Informação, que responde matricialmente à Diretoria Executiva.

PROPRIEDADE INTELECTUAL

A propriedade intelectual é a proteção que recai sobre bens imateriais, tais como: marcas, sinais distintivos, slogans publicitários, nomes de domínio, nomes empresariais, indicações geográficas, desenhos industriais, patentes de invenção e de modelo de utilidade, obras intelectuais (tais como obras literárias, artísticas e científicas, base de dados, fotografias, desenhos, ilustrações, projetos de arquitetura, obras musicais, obras audiovisuais, textos e etc.), programas de computador e segredos empresariais (inclusive segredos de indústria e comércio).

Pertencem exclusivamente a VIPE todas e quaisquer invenções, criações, obras e aperfeiçoamentos que tenham sido ou venham a ser criados ou

realizados pelo colaborador a VIPE, na qualidade de administrador, empregado e/ou estagiário, durante todo o prazo de vigência do mandato, contrato de trabalho ou contrato de estágio do colaborador. Quaisquer informações e conteúdos cuja propriedade intelectual pertença a VIPE, ou tenham sido por ela disponibilizados, inclusive informações e conteúdos que tenham sido obtidos, inferidos ou desenvolvidos pelo próprio colaborador em seu ambiente de trabalho ou utilizando recursos da instituição não devem ser utilizados para fins particulares, nem repassados a terceiros, sem autorização prévia e expressa da VIPE.

É dever de todos os colaboradores zelar pela proteção da propriedade intelectual da VIPE.

DECLARAÇÃO DE RESPONSABILIDADE

Todos os colaboradores da VIPE devem aderir formalmente a um termo, comprometendo-se a agir de acordo com as políticas de Segurança da Informação.

Os contratos firmados com a VIPE devem possuir cláusula que assegure a confidencialidade e exclusividade das informações.

PAPÉIS E RESPONSABILIDADES

As políticas, estratégias e processos corporativos de Segurança da Informação e Segurança Cibernética são supervisionados pela Gerência de Tecnologia da Informação e discutidos nos fóruns específicos de riscos das áreas e nas Comissões Executivas que tratam Risco Operacional ou Tecnologia.

Departamento de Tecnologia da Informação

O Departamento de Tecnologia da Informação tem a função de manter o parque tecnológico disponível e atualizado, com os padrões de segurança implementados, dentro dos prazos compatíveis com os níveis de riscos.

Além disso, o Departamento de Tecnologia da Informação também é composto pelas áreas de Segurança da Informação e Segurança Cibernética e pelos Comitês de Segurança Corporativa (Governança de TI) e de Auditoria em Segurança da Informação, conforme listados em tópico acima. Tal área e comitês possuem as seguintes atribuições:

Segurança da Informação e Segurança Cibernética

São atribuições da referida área:

- Aprimorar a qualidade e efetividade de seus processos, buscando a integridade, disponibilidade e confidencialidade das informações;
- Proteger a informação de ameaças buscando garantir a continuidade do negócio e minimizar os riscos ao negócio;
- Estabelecer, implementar, operar, monitorar e garantir a melhoria contínua do sistema de gestão de segurança da informação.
- Definir e formalizar os objetivos, controles e a estratégia de governança de segurança da informação, em conjunto com o Comitê de Segurança Corporativa (Governança de TI).
- Coordenar as ações para atingimento dos objetivos e da estratégia de governança de segurança da informação aprovados pelos comitês, envolvendo as áreas responsáveis.
- Estabelecer e disseminar uma cultura de segurança da informação.
- Propor o investimento para a segurança da informação.
- Definir as políticas e padrões de segurança da informação a serem aplicados nos processos, produtos e tecnologias.

Comitê de Segurança Corporativa

O Comitê de Segurança Corporativa tem por atribuição aprovar a estratégia, objetivos, orçamento e ações necessárias para a mitigação dos riscos dos processos de segurança da informação.

Comitê de Auditoria em Segurança da Informação

O Comitê de Auditoria deverá supervisionar os processos de segurança da informação.

Auditoria Interna

Os papéis e responsabilidades da Auditoria Interna estão descritos na Política de Auditoria Interna.

Áreas de Negócios

As Áreas de Negócios devem proteger as informações da VIPE Financeira sob sua responsabilidade.

SANÇÕES DISCIPLINARES

As violações a esta Política estão sujeitas às sanções disciplinares previstas nas políticas internas, notadamente no Manual de Boas-Vindas e Código de Conduta, e na legislação vigente.

DOCUMENTOS RELACIONADOS

Esta Política é complementada por manuais e procedimentos específicos de Segurança da Informação, em conformidade com os aspectos legais e

regulamentares e aprovadas pela área de Segurança da Informação e Segurança Cibernética e pelo Comitê de Segurança Corporativa.

VIGÊNCIA E ATUALIZAÇÃO

Esta Política entra em vigor na data de sua aprovação e será revisada anualmente e alterada quando necessário, sem aviso prévio. As alterações serão divulgadas a todos os colaboradores, parceiros e correspondentes da VIPE, por e-mail, e ficarão disponíveis para consulta website da instituição, bem como na Intranet.

GLOSSÁRIO

APT (Advanced Persintent Threat): ataques avançados persistentes.

Cyber Security: é o termo que designa o conjunto de meios e tecnologias empregadas na defesa dos sistemas de informação, infraestrutura, redes de computadores e/ou dispositivos pessoais, com o objetivo de prevenir danos, roubo, intrusão, alterações ou destruição de informações.

Parque tecnológico: conjunto de ativos de infraestrutura e sistemas de tecnologia.

Segregação de funções: consiste na separação das atividades entre áreas e pessoas potencialmente conflitantes ou que possuem informações privilegiadas, na qual, o colaborador não pode exercer mais que uma função nos processos de autorização, aprovação, execução, controle e contabilização.

CANAIS DE COMUNICAÇÃO DE SEGURANÇA DA INFORMAÇÃO

- Recebeu um e-mail suspeito e deseja enviá-lo para análise? Encaminhe e-mail para: compliance@somosvipe.com.br

- Suspeitas de incidentes de segurança da informação? Encaminhe e-mail para: ti@somosvipe.com.br

São Paulo, 15 de dezembro de 2023

Aprovada por: FERNANDO CARNEIRO FERRAZ DE ANDRADE:29885184830

Assinado de forma digital por FERNANDO CARNEIRO FERRAZ DE ANDRADE:29885184830
Dados: 2023.12.22 15:37:19 -03'00'

Fernando Ferraz – Diretor Presidente

Elaborado por:

Daniel Goivinho Pezybyn – Jurídico e Compliance

Talita Goulart Verdasca - Compliance

DANIEL GOIVINHO PEZYBYN

Assinado de forma digital por DANIEL GOIVINHO PEZYBYN
Dados: 2023.12.22 16:43:07 -03'00'