SEGURANÇA CIBERNETICA

Título	**Política de Segurança Cibernética**
Código	**POL00024**
Tipo	**Política**
Versão	**2ª Versão**
Data de vigência	**maio/25 – maio/26**
Área responsável	**Tecnologia e Segurança da Informação**
Aprovação	**Everson Gonçalves Ramos e Ricardo Fuscaldi Baptista**

ÍNDICE

DEFINIÇÕES

BCB	Banco Central do Brasil
CMN	Conselho Monetário Nacional
Colaboradores	Empregados e Administradores do Grupo Vórtx
CVM	Comissão de Valores Mobiliários
ISO 27001	A norma ISO 27001 é o padrão e a referência internacional para a gestão da segurança da informação
Lei nº 13.709/2018 ou LGPD	Lei Geral de Proteção de Dados
NIST – Cyber Security Framework	Conjunto de diretrizes para mitigar os riscos de segurança cibernética organizacional, publicado pelo Instituto Nacional de Padrões e Tecnologia dos EUA, com base em padrões, diretrizes e práticas existentes
Parceiros	Pessoa física ou jurídica que decide oferecer, e/ou prestar serviços determinados em contrato com quaisquer das empresas do Grupo Vórtx
Resolução BCB nº 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 autorizadas a funcionar pelo Banco Central do Brasil.
Vórtx e/ou Grupo Vórtx	Grupo de empresas vinculadas societariamente e sob o controle comum, direta ou indiretamente, da Vértera Holding S.A.

1. ASPECTOS GERAIS

1.1 Objetivo

Este Normativo trata as diretrizes e controles sobre Segurança Cibernética do Grupo Vórtx. Esse documento também dever ser utilizado para comunicação dos clientes e visitantes de que a Vórtx cuida da confidencialidade e privacidade dos seus dados tanto quanto da disponibilidade e integridade dos sistemas e informações prestadas pela instituição.

As diretrizes têm por objetivos principais:

(i) Orientar os clientes e visitantes sobre quais são e como minimizar os riscos digitais em seus acessos aos sistemas e sites da Vórtx;

(ii) Estabelecer as diretrizes de cibersegurança, visando proteger os ativos de tecnologia e os dados dos clientes;

(iii) Informar as áreas e atribuir responsabilidades para cumprimento da Política e garantir a segurança da informação; e,

(iv) Garantir a conformidade com os requisitos da Resolução BCB nº 85/2021, especialmente no que tange à estrutura de governança, processos de avaliação e mitigação de riscos cibernéticos, e tratamento de incidentes de segurança da informação

(v) Dar ciência ao público, quanto as iniciativas de cibersegurança da companhia.

1.2 Relacionamento do Normativo com outros documentos

Esta Política deve ser lida e interpretada em conjunto com o Código de Ética e Conduta e demais políticas e procedimentos internos:

(i) Política de Privacidade da Vórtx;

(ii) Termos de Uso;

(iii) Resolução BCB nº 85/2021LGPD;

(iv) ISO 27001;

(v) NIST – Cyber Security Framework;

(vi) Politica de Segurança da Informação

(vii) Política de Continuidade de Negócios e Plano de Recuperação de Desastres;

(viii) Plano de Resposta a Incidentes Cibernéticos

2. DISPOSIÇÕES GERAIS

Ao estabelecer princípios e diretrizes de Segurança Cibernética, a Vórtx busca assegurar a confidencialidade, integridade e a disponibilidade dos ativos físicos e lógicos de informação da companhia, para garantir que os requisitos legais, contratuais e operacionais sejam honrados.

A Vórtx deposita seus maiores esforços para prover uma proteção adequada para os ativos e dados, garantindo a identificação, proteção, detecção, resposta e recuperação em caso de eventuais incidentes de segurança da informação.

2.1 Riscos de operações digitais (via *Internet*)

Dentre os motivadores para que os ataques cibernéticos sejam realizados, estão:

(i) Obter ganhos financeiros;

(ii) Roubar, manipular ou adulterar informações;

(iii) Fraudar, sabotar ou expor a instituição invadida, visando gerar impacto à marca;

(iv) Obter vantagens competitivas e informações confidenciais de empresas concorrentes;

(v) Praticar atos de terror e disseminar pânico e caos; e

(vi) Enfrentar desafios e/ou fornecer serviços para hackers com intenção de expor e causar danos à marca ou por admiração a fraudadores famosos.

Os invasores podem utilizar vários métodos para ataques na rede mundial de computadores, sendo os mais comuns:

- **Malware** – é um software usado ou programado por atacantes (hackers) para interromper a operação normal de um dispositivo, coletar informações confidenciais, tomar o controle total ou obter acesso a sistemas e informações. Malware é um termo geral usado para se referir a uma variedade de softwares hostis ou intrusivos, incluindo:
- **Vírus**: Software que causa danos ao computador, rede, softwares e banco de dados;
- **Cavalo de Troia**: aparece dentro de outro software e cria uma porta de entrada para o invasor controlar o computador;
- **Spyware**: software malicioso utilizado para coletar e monitorar o uso de informações;
- **Keylogger**: software malicioso que registra as informações digitadas e envia ao hacker; e
- **Ransomware**: software malicioso que bloqueia e sequestra os dados, sejam sistemas ou bases de dados, e é solicitado um resgate para que o acesso seja reestabelecido e que pode não ocorrer mesmo após pagamento.
- **Engenharia Social** – método de manipulação, utilizado para obter informações confidenciais,

como senhas, dados pessoais, número de cartão de crédito e segredos comerciais valiosos que incluem propostas comerciais e contratos, listas de clientes ou fornecedores, além de informações financeiras e planos financeiros.

- **Phishing**: links transmitidos por e-mail, simulando ser uma pessoa ou uma empresa confiável que realiza o envio de comunicações eletrônicas oficiais para obter informações confidenciais, ou obrigar que o usuário execute transações por seu senso de urgência.
- **Spoofing**: essa ameaça tem como princípio a falsificação de endereços de e-mails, IPs e DNS, em que o cibercriminoso cria uma fonte de IP que pareça confiável, modifica o cabeçalho de um e-mail para parecer legítimo ou alterar o DNS, com o intuito de redirecionar um nome específico para um domínio alternativo.
- **Pharming**: direciona o usuário para sites fraudulentos, sem seu conhecimento;
- **Smishing**: simula ser uma pessoa ou empresa confiável e, por meio de mensagens de texto, tenta obter informações e dados confidenciais;
- **Vishing**: é uma técnica utilizada por cibercriminosos e fraudadores para conseguir aplicar golpes por telefone, se passando por pessoas confiáveis que possuem informações reais sobre clientes das instituições. O vishing usa de golpes verbais para induzir pessoas a realizarem atos que elas acreditam ser de seu real interesse, e em geral o vishing começa no ponto em que termina o phishing.
- **Acesso pessoal**: pessoas localizadas em ambientes públicos como bares, restaurantes, cafés e elevadores que captam informações que de alguma forma podem ser utilizadas posteriormente para um ataque.
- **Ataques de DDoS (Distributed Denial of Services) e botnets**: também conhecido como ataque de negação de serviço distribuído, é uma modalidade de ataque utilizada para tentar indisponibilizar um site, sistema ou recurso de rede enviando milhares de requisições com tráfego mal-intencionado, deixando a estrutura incapaz de operar. Já no caso dos botnets, o ataque vem de muitos computadores infectados utilizados para criar e mandar spam ou vírus, ou inundar uma rede com mensagens, resultando na negação de serviços. Botnets são conhecidos como bots ou computadores zumbis, sendo que alguns desses bots podem conter milhares de computadores.

2.2 Medidas e controles adotados na Vórtx

A Vórtx controla os dados, sistemas e serviços, com o objetivo de proteger seus ativos de informação e a privacidade de seus clientes contra coleta, retenção, uso, divulgação, alteração ou destruição não

autorizada. Os temas são abordados por meio de políticas, normas, procedimentos internos e arquitetura de segurança com adoção dos controles apropriados. Dado isso, as medidas de segurança cibernética adotadas pela Vórtx, previstos na presenta Politica, estão alinhadas aos requisitos do art. 5º da Resolução BCB nº 85/2021 e abrangem os seguintes controles:

- **Programa de Treinamento e Conscientização de Segurança da Informação e Riscos Cibernéticos -** periodicamente é aplicado o programa de conscientização de segurança aos Colaboradores, Terceiros, estagiários e menores aprendizes, a fim de que todos tenham conhecimento quanto aos riscos e formas de agir adequadamente nos diversos cenários apresentados. Os documentos internos, sejam eles políticas ou normas, garantem os deveres e responsabilidades de todos os colaboradores em relação à proteção dos ativos da Vórtx.
- **Controle de Acesso –** Todo o acesso é concedido com base em perfis de usuário e com aprovação prévia adequada e seguem as seguintes premissas: (i) "**necessidade de saber**", indica que o usuário tem um motivo legítimo para acessar algo; e (ii) **"mínimo privilégio"**, é o nível de permissão que limita o acesso a algo que o usuário pode ou não fazer. Adicionalmente, o acesso a dispositivos móveis e serviços de armazenamento web também são controlados.
- **Segmentação de Ambiente –** A infraestrutura dos ambientes é segregada para que exista um melhor controle de tráfego entre eles, garantindo restrições nos ambientes que exigem segregação de dados produtivos, testes e homologação, bem como as devidas confidencialidade e integridade aos dados e informações.
- **Segurança nas Aplicações –** Desde o processo de planejamento e criação da arquitetura, até a implantação, todas as aplicações estão sujeitas a um processo de análise de segurança para confirmar que estas foram desenvolvidas de acordo com as políticas vigentes e práticas padrões de segurança para desenvolvimento de aplicações.
- **Plano de Continuidade de Negócio e Recuperação de Desastres –** A infraestrutura tecnológica do Grupo Vórtx é em cloud e sua operação totalmente digital, arquitetado para que os sistemas, processos e ativos suportem eventos de todas as naturezas, utilizando de recursos de alta disponibilidade que visam garantir contingência até mesmo em território internacional, se necessário. Os sistemas e bases de dados que mantem disponibilidade, são testados para garantir a continuidade das operações em casos de desastres reais. São realizadas novas análises de impacto ao negócio e alterações no plano caso necessário.

- **Gestão de Fornecedores –** É o processo conduzido por meio de análises e diligências em atividades relacionadas às áreas de Segurança da Informação, Legal, Compliance e Riscos, quando da contratação de uma plataforma, sendo avaliados neste processo:

(i) Diretrizes de segurança do fornecedor;

(ii) Controles em relação à Privacidade dos Dados;

(iii) Revisões de diligência, classificação de risco, resultados e parecer de segurança quanto a contratação;

(iv) Avaliação de potenciais fornecedores quantos as melhores práticas de segurança da informação e segurança da plataforma oferecida; e

(v) Mitigação de Riscos e inclusão de planos de ação.

- **Resposta a Incidentes –** A área de Segurança da Informação detecta, controla e remedia os incidentes relacionados à segurança de sistemas, processos e ativos de informação. Em caso de violações, notificações oportunas a clientes afetados são emitidas de acordo com os requisitos contratuais, regulamentares e legislativos. Periodicamente são feitas revisões e novas análises do processo (plano de resposta a incidentes) para garantir a eficiência na detecção, controle e contensão dos incidentes. Todos os incidentes relevantes são documentados e analisados conforme critérios estabelecidos pela Resolução BCB nº 85/2021, com comunicação tempestiva ao Banco Central do Brasil, quando aplicável.
- **Proteção de Marca:** O Grupo Vórtx conta com uma solução de proteção de riscos digitais, que mantem a vigilância em todo ambiente tecnológico, desde a surface até a darkweb. A plataforma contratada tem como objetivo principal ajudar na proteção contra ameaças externas, monitoramento e detecção contínua ativos expostos, além de fornecer formas de mitigar e erradicar os riscos.
- **Processo de Gestão de Vulnerabilidade –** A Vórtx adota com regularidade rotinas que visam mitigar as falhas sistêmicas que podem ser exploradas por atacantes. Todas as falhas detectadas são registradas para acompanhamento e correção, de acordo com o nível de criticidade, seja para sistemas, softwares e hardwares.
- **Proteção de Recursos Computacionais –** Os equipamentos e demais recursos de tecnologia da Vórtx possuem regras e políticas de configuração segura, patches de segurança com atualizações constantes e proteção contra malwares. Todo o tráfego de dados, rede e mídias são controlados e monitorados, por meio de softwares reconhecidos de mercado.
- **Procedimento e Controles Internos –** a área de Segurança da Informação está sujeita a

processos de auditoria, avaliações de controles internos e testes de conformidade de forma periódica, além de contar com a estrutura de Compliance para aderência às normas e circulares de órgãos reguladores e autorreguladores do mercado.

- **Teste de Intrusão –** são realizados testes periódicos nas estruturas tecnológicas do Grupo Vórtx. É feita a simulação de ataques, executado por um hacker ético de empresa externa e, após a conclusão do processo, as falhas e vulnerabilidades encontradas são tratadas e corrigidas.

A Vórtx mantém um processo de auditoria e revisão periódica dos controles de segurança cibernética, com base em testes de vulnerabilidade, simulações de ataque e avaliação contínua dos riscos cibernéticos.

2.3 Práticas de Segurança para clientes e visitantes:

(i) Mantenha seus dados atualizados;

(ii) Mantenha sigilo das suas informações pessoais. Não realize cadastros em sites que não transmitam segurança ou que seus dados possam ficar desprotegidos, bem como em sites que solicitem mais informações do que é necessário para executar o serviço;

(iii) Proteja sua estação de trabalho contra malwares. Mantenha seu sistema operacional atualizado e com as correções de segurança;

(iv) Tenha uma ferramenta de proteção contra malwares;

(v) Cuidado ao visitar sites, faça visita e utilize sites e serviços confiáveis;

(vi) Não faça download de nenhum arquivo, programa ou software em sites desconhecidos ou suspeito, e não instale no seu computador;

(vii) Busque por canais oficiais do fabricante de softwares e programas para fazer download e posterior instalação;

(viii) Cadastre uma senha forte e utilize um segundo fator de autenticação;

(ix) Tenha sempre cuidado para abrir arquivos e links recebidos por e-mail, pode ser um phishing;

(x) Não reutilize suas senhas e outros sites e aplicativo; e

(xi) Caso suspeite de alguma conduta ou ações incomuns, busque imediatamente o canal oficial de relacionamento com o cliente da Vórtx.

3. GOVERNANÇA

3.1 Alta Administração

A Alta Administração se compromete com a melhoria contínua dos processos e recursos necessários

para a Segurança Cibernética, de acordo com os objetivos e estratégias do negócio, em conjunto com as leis e regulamentações vigentes, bem como asseguram o cumprimento desta Política.

A Alta Administração é responsável por aprovar, revisar anualmente e garantir a implementação das estratégias de segurança cibernética, em conformidade com a Resolução BCB nº 85/2021.

3.2 Área de Operações Tecnologia e Segurança da Informação

A área de Operações Tecnologia e Segurança da Informação, possui as seguintes funções e responsabilidades:

(i) Manter os processos e controles descritos nessa Politica;;

(ii) Proteger as informações confidenciais e sensíveis da Vórtx, contra acessos indevidos e não autorizados;

(iii) Manter sistemas, softwares e plataformas de segurança atualizados e com as últimas correções;

(iv) Reportar e comunicar incidentes de segurança e/ou violações aos órgãos reguladores e/ou a clientes, quando necessário;

(v) Proteger dispositivos e mídias que contenham informações sensíveis;

(vi) Disseminar a cultura de segurança da informação através do programa de conscientização;

(vii) Revisar e manter esta Politica atualizada;

(viii) Manter a alta disponibilidade do ambiente tecnológico;

(ix) Mitigar riscos e incidentes de segurança cibernética; e

(x) Implementar e operar um processo contínuo de identificação, avaliação e tratamento de riscos cibernéticos, conforme diretrizes da Resolução BCB nº 85/2021.

(xi) Manter seu ambiente tecnológico íntegro.

3.3 Comitê de Riscos e Compliance

O Comitê de Riscos e Compliance possui às seguintes atribuições:

- ✓ Determinar as políticas gerais de proteção de dados e segurança da informação da Vórtx;
- ✓ Aprovar métricas e relatórios de proteção de dados e segurança da informação, com o intuito de assessorar nas decisões estratégicas da Vórtx;
- ✓ Definir prioridades e determinar medidas pertinentes à proteção de dados e segurança da informação de acordo com os insumos fornecidos pela diretoria de tecnologia; e
- ✓ Supervisionar a atuação e o desempenho das áreas responsáveis quanto a referida Política.

4. VIGÊNCIA E ATUALIZAÇÃO

O documento será revisado anualmente, ou quando constatada a necessidade de atualização do seu conteúdo. Poderá, ainda, ser alterado a qualquer tempo em razão de circunstâncias que demandem tal providência. Vale destacar que a revisão observará a necessidade de atualização, conforme evolução dos riscos cibernéticos e exigências regulatórias.

Data	Versão	Responsável	Motivo da alteração
11 de dezembro de 2023	1ª	Segurança da Informação	Elaboração
27 de maio de 2025	2ª	Segurança da Informação	Revisão