POLÍTICA

SEGURANÇA CIBERNÉTICA

vtreo

Data	Versão	Autor	Aprovação	Observações
Setembro/2019	1.0	Segurança da Informação	Diretoria	Não se aplica.
Agosto/2022	2.0	Segurança da Informação	Diretoria	Atualização Itens 1, 3 e 6.2.

1. APRESENTAÇÃO

A Vitreo Distribuidora de Títulos e Valores Mobiliários S.A., denominada neste documento como "Vitreo DTVM", é uma instituição autorizada a funcionar pelo Banco Central do Brasil ("BCB") e pela Comissão de Valores Mobiliários ("CVM"). O seu foco de atuação é em distribuição e custódia de ativos.

A Vitreo Gestão de Recursos Ltda., por sua vez, denominada neste documento como "Vitreo Gestão", é uma instituição autorizada a funcionar pela Comissão de Valores Mobiliários e o seu foco de atuação é a gestão de carteira de valores mobiliários.
A Vitreo DTVM e a Vitreo Gestão são denominadas em conjunto como "Grupo Vitreo" neste documento.

2. OBJETIVO

Este documento trata as diretrizes e controles sobre Segurança Cibernética do Grupo Vitreo. Esse documento também dever ser utilizado para comunicar aos seus clientes e visitantes de que a Vítreo cuida da Confidencialidade e Privacidade dos seus dados tanto quanto da disponibilidade e integridade dos nossos sistemas e informações prestadas.

As diretrizes têm por principais objetivos:

- Orientar os clientes e visitantes sobre quais são e como minimizar os riscos digitais em seus acessos ao sistemas e sites da Vítreo;
- Demonstrar como a Vítreo é diligente para proteger os ativos de informação;
- Servir de referência para auditorias, verificações de conformidade e determinação de responsabilidades.

3. VIGÊNCIAS E ATUALIZAÇÕES

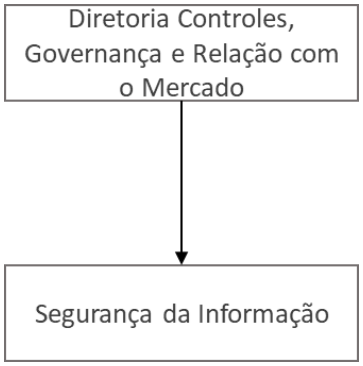
As diretrizes contidas nesta Política entram em vigor na data de sua publicação e permanecem vigentes por prazo indeterminado, devendo ser revisadas 24 meses ou em prazo inferior, sempre que solicitado pelo órgão regulador, em casos de alteração de legislação aplicável ou ainda, se houver alteração no modelo de negócios, previamente validado pelo Compliance.

A aprovação desta Política e posterior atualizações deverão ser realizadas por todos os Diretores da Vitreo DTVM, com a aprovação registrada em ata assinada.

4. REGULAMENTAÇÃO APLICÁVEL

- Lei 9.609/98;
- Resolução CMN n° 4.893/21

5. ESTRUTURA DA ÁREA



6. DISPOSIÇÕES GERAIS

6.1 RISCOS DE OPERAÇÕES DIGITAIS (pela Internet)

Existem diversas razões para que esses ataques sejam realizados. Os principais motivos identificados são:

- Obter ganho financeiro.
- Roubar, manipular ou adulterar informações.
- Obter vantagens competitivas e informações confidenciais de empresas concorrentes.
- Fraudar, sabotar ou expor a instituição invadida, podendo ter como motivo acessório a vingança.

- Promover ideias políticas e/ou sociais.
- Praticar o terror e disseminar pânico e caos.
- Enfrentar desafios e/ou ter adoração por hackers famosos.

Os invasores podem utilizar vários métodos para os ataques cibernéticos. Destacam-se os mais comuns:

- **Malware** – é um software usado ou programado por atacantes para interromper a operação do computador, coletar informações confidenciais ou obter acesso a sistemas de informação. Malware é um termo geral usado para se referir a uma variedade de formas de software hostil ou intrusivo, incluindo:
    - **Vírus:** software que causa danos a máquina, rede, softwares e banco de dados;
    - **Cavalo de Troia:** aparece dentro de outro software e cria uma porta para a invasão do computador;
    - **Spyware:** software malicioso para coletar e monitorar o uso de informações; e
    - **Ransomware:** software malicioso que bloqueia o acesso a sistemas e bases de dados, solicitando um resgate para que o acesso seja reestabelecido.
- **Engenharia social** – métodos de manipulação para obter informações confidenciais, como senhas, dados pessoais e número de cartão de crédito:
    - **Pharming:** direciona o usuário para um site fraudulento, sem o seu conhecimento;
    - **Phishing:** links transmitidos por e-mails, simulando ser uma pessoa ou empresa confiável que envia comunicação eletrônica oficial para obter informações confidenciais;
    - **Vishing:** simula ser uma pessoa ou empresa confiável e, por meio de ligações telefônicas, tenta obter informações confidenciais;
    - **Smishing:** simula ser uma pessoa ou empresa confiável e, por meio de mensagens de texto, tenta obter informações confidenciais; e
    - **Acesso pessoal:** pessoas localizadas em lugares públicos como bares, cafés e restaurantes que captam qualquer tipo de informação que possa ser utilizada posteriormente para um ataque.
- **Ataques de DDoS ("Distributed Denial of Services") e botnets** – ataques visando negar ou atrasar o acesso aos serviços ou sistemas da instituição; 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. número de computadores infectados utilizados para criar e mandar spam ou vírus, ou inundar uma rede com mensagens resultando na negação de serviços.
- **Invasões –** ataques realizados por invasores sofisticados, utilizando conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico.

6.2 DILIGÊNCIAS E CONTROLES DA VITREO

A Vítreo controla os dados, sistemas e serviços, com o objetivo de proteger os ativos de informações e a privacidade de seus clientes contra a coleta, retenção, uso, divulgação, modificação ou destruição não autorizada. Isso é abordado através de normas, procedimentos e arquitetura de segurança com a adoção de controles técnicos apropriados. A política e os controles de segurança da informação fornecem cobertura de áreas críticas de segurança da informação, incluindo:

- **Programa de Conscientização de Segurança da Informação e Riscos Cibernéticos –** Periodicamente é feito um programa de conscientização de segurança aos funcionários e demais colaboradores para que conheçam os riscos e possam agir adequadamente. As políticas de segurança garantem os deveres e responsabilidades dos funcionários e demais colaboradores em relação à proteção dos ativos de informação.
- **Controle de acesso -** O acesso é concedido com um mínimo de privilégio e necessidade de saber. Todo o acesso é concedido com base em perfis de usuários e com aprovação prévia adequada. Acesso a dispositivos moveis e serviços de armazenamento web são controlados.
- **Segmentação dos Ambientes –** Os ambientes são segregados para que exista um controle de trafego entre os eles, garantindo maior restrição nos ambientes que exigem mais integridade e confidencialidade.
- **Segurança de aplicações –** Desde o processo de planejamento e criação da arquitetura, até o processo de implantação, as aplicações estão sujeitas a um processo de análise de segurança para confirmar que foram desenvolvidas de acordo com nossas normas e padrões de segurança de desenvolvimento de aplicativos.
- **Classificação das Informações –** Todas as informações geradas ou sobre custódia pela Vítreo, são classificadas de forma manual ou automática (quando possível) de acordo com as normas internas de classificação a informação, garantido o nível de proteção adequado a informação.
- **Plano de Continuidade ao Negócio e Recuperação de Desastres –** O ambiente Operacional da Vítreo é digital, arquitetado para que os sistemas, processos e ativos críticos suportem eventos catastróficos utilizando de recursos em alta disponibilidade, garantindo contingência até mesmo em nível internacional, caso se faça necessário. Os sistemas que mantem essa disponibilidade são testados regularmente para garantir a eficácia do processo em casos reais de desastres. São feitas regularmente novas análises de impacto ao negócio e alterações no plano caso se façam necessário.
- **Gerenciamento de Fornecedores** – O processo conduz análises de diligências em atividades relacionadas à Segurança da Informação e Compliance de terceiros, incluindo:
    - Avaliação de potenciais fornecedores para o cumprimento das políticas e controles da empresa;
    - Controles em relação a Privacidade dos Dados;
    - Revisões de devida diligência, incluindo a elaboração de classificações de risco e resultados;

- Mitigação de riscos;
- Suporte na seleção de fornecedores.

- **Resposta a Incidentes –** O departamento de Segurança da Informação detecta, controla e remedia incidentes relacionados a segurança de sistemas, processos e ativos de informação.

  Em caso de alguma violação, a equipe de segurança da informação tomará medidas para manter as informações seguras e mitigar a violação. As notificações oportunas de clientes afetados são emitidas de acordo com os requisitos contratuais, regulamentares e legislativos.
  Periodicamente são feitas novas análises deste processo (plano) para garantir máxima eficiência na detecção e controle dos incidentes.

- **Gestão de Vulnerabilidades –** É feito regularmente processos de rotina que visem diminuir as falhas sistêmicas que possam ser exploradas por ataques. Todas as falhas detectadas são colocadas para acompanhamento e correção de acordo com o nível de criticidade do sistema.

- **Proteção de Recursos Computacionais –** Todos equipamentos computacionais da Vítreo, possuem políticas de configuração segura, atualizações constantes de patches de segurança e proteções contra malwares. Todos tráfegos de rede e mídias removíveis são controlados e monitorados para detecção de incidentes.

6.3 BOAS PRÁTICAS DE SEGURANÇA PARA OS CLIENTES E VISITANTES

- Tenha cuidado com mensagens de e-mail fraudulentas, se atente aos detalhes, como endereço do remetente está correto, domínio, links suspeitos no corpo do e-mail;
- Mantenha sigilo das suas informações pessoais. Não deixe ela em lugares que considere desprotegidos ou aberto para que outros possam ter;
- Proteja sua estação de trabalho contra malwares. Mantenha sempre o seu sistema operacional atualizado com as correções de segurança e possua uma ferramenta contra malwares;
- Visite somente sites confiáveis. Visite apenas sites confiáveis e não faça download de nenhum arquivo ou programa de sites desconhecidos ou suspeitos. Tenha sempre cuidado ao abrir um arquivo desconhecido ou ao clicar em links suspeitos; e
- Certifique-se que o código de autenticação enviados via sms ou e-mail (segundo fator), são enviados para o endereço de e-mail (ou telefone) que somente você possua o acesso e de forma segura.

7. DIVULGAÇÃO DAS POLÍTICAS E DOCUMENTOS ACESSÓRIOS

Regras gerais para a divulgação da política, de forma a permitir livre acesso e ciência por todos os cobertos pelo seu manto, mantendo a consistência e atualidade dos documentos diante de mudanças.

É implementado um controle de versões online da política e dos documentos acessórios associados quando aplicavel.

8. MANUTENÇÃO DOS ARQUIVOS

O Grupo Vitreo manterá armazenado todos os arquivos eletronicamente, pertinentes ao processo de Conformidade desta política por prazo mínimo de 05 (cinco) anos, conforme legislação vigente.