POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

VANQUISH ASSET MANAGEMENT

Março, 2023

VANQUISH

Asset Management

1. Objetivo

Esta política (“Política”) visa estabelecer os procedimentos para manter a proteção e segurança das informações em posse da Vanquish, bem como regras, procedimentos e controles para o tratamento adequado no que se refere à segurança cibernética (cibersegurança), de acordo com a legislação vigente.

2. Aplicabilidade

Esta Política é aplicável a todos os colaboradores da Vanquish, sócios e/ou colaboradores, bem como a todos os prestadores de serviços que possuem vínculo com a gestora.

3. Estrutura

A Vanquish conta com um Diretor e dois profissionais de tecnologia. Tal estrutura está preparada para eventuais paralisações decorrentes de queda de energia entre outras contingências que possam vir à ocorrer.

4. Infraestrutura

A Vanquish busca adotar tecnologias de segurança da informação com o objetivo de impedir:

- Acesso e/ou transmissão de informações e/ou arquivos confidenciais para pessoas não autorizadas;
- Liberação de senhas e códigos de identificação de usuários; e
- Ocorrência de ataques cibernéticos.

Para a rastreabilidade da informação no sentido de buscar garantir a segurança das informações sensíveis a Vanquish.

5. Atribuição da Diretoria de Tecnologia e Segurança da Informação

- Monitora os *logs* de acesso para identificar atipicidades nos perfis de acesso dos usuários;
- Disponibiliza acessos restritos aos colaboradores que utilizam dados sensíveis, seja de pessoa física ou jurídica, nos termos das legislações vigentes;
- Mantém os equipamentos e as instalações de processamento de informação críticas ou em áreas seguras, com níveis e controles de acesso apropriados, incluindo proteção contra ameaças físicas e ambientais;
- Mantém *softwares* especializados de segurança para a proteção da infraestrutura contra ameaças, como: *firewall*, antivírus, antispam;
- Bloqueia as de portas USB e dos gravadores de mídia em todos os computadores,
- Realiza testes periódicos nos equipamentos utilizados pela Vanquish;
- Disponibiliza recursos, equipamentos e *softwares* adequados para a função do colaborador;
- Mantém ferramentas de monitoramento com registro de acessos à rede de gravação de voz dos ramais da Vanquish;
- Disponibiliza acesso seguro aos colaboradores autorizados;
- Mapeia as atividades consideradas críticas e essenciais para a continuidade dos negócios;
- Registra as ocorrências ocorridas, visando evitar reincidência e/ou novos incidentes.

6. Atribuição do Diretor de Riscos, Compliance e PLD/FTP

O Diretor de Riscos, Compliance e PLD/FTP, sempre que formalizar, deverá ter acesso irrestrito à dados sigilosos e/ou protegidos por lei. No entanto, deverão acessar tais dados de forma diligente e sigilosa, à luz das legislações vigentes que exigem a coleta de informações sobre clientes, colaboradores, parceiros e fornecedores, no âmbito das análises de Compliance – PLD/FTP.

7. Controles adotados pela Vanquish

- Autenticação por *login* e senha com grau de complexidade e criptografia;
- Bloqueio de acesso a gravadores com monitoramentos realizados pela área de tecnologia;
- Realização de testes periódicos e varreduras visando identificar vulnerabilidades, por meio dos sistemas de antivírus e *firewall*;
- Mecanismos de rastreabilidade por meio das trilhas de auditorias e *logs* de eventos;
- Controles de acesso e de segmentação da rede de computadores em ambientes, diretórios e arquivos específicos e segregados;
- Manutenção de cópias de segurança dos dados e das informações por *backups* com testes periódicos de integridades nas cópias;
- O acesso como administrador aos sistemas de informações, plataforma em nuvem e à infraestrutura interna são restritos ao Diretor e à um colaborador da área de TI.
- O acesso de visitantes às instalações da Vanquish deverá ser previamente aprovado pelo Diretor responsável pela área a ser visitada, com apresentação de documento de identificação.

8. Recomendações, Orientações e Vedações

- As senhas são secretas, pessoais e intransferíveis, sendo expressamente proibido o compartilhamento das mesmas com terceiros;
- Alterar as senhas periodicamente visando mitigar riscos;
- Por segurança, é necessário o bloqueio dos computadores ao ausentar-se;
- É vedado o armazenamento de senhas ou informações confidenciais em locais que possam ser visualizados por terceiros, sendo obrigatório manter a estação de trabalho organizada;
- Descartar, adequadamente, papéis, materiais físicos ou eletrônicos confidenciais para inviabilizar acessos por terceiros;
- Colaboradores desligados devem ter todo e quaisquer acessos tempestivamente bloqueados;
- Colaboradores que tenham conhecimento ou possuam acesso indevido ou informação de dados sensíveis, devem, tempestivamente, comunicar ao Diretor de Compliance, Riscos e PLD/FTP;
- É vedado utilizar qualquer forma de acesso externo ou conexão com os equipamentos internos da Vanquish, como forma de minimizar o risco de roubo de informações ou contaminações dos sistemas.

9. Incidentes

Visando a prevenção e tratamento dos incidentes, caso ocorram, os fornecedores e prestadores de serviços contratados pela Vanquish deverão assinar um termo de Confidencialidade das Informações.

10. Infraestrutura Tecnológica

A Vanquish conta com serviço de mensagens de e-mail da Microsoft, solução *Exchange Online*, garantida por meio de certificado SSL para suas portas de acesso. Desta forma, todos os e-mails enviados pelo domínio da Vanquish seguem criptografados até o seu destinatário, evitando possíveis perdas ou furto de informações.

São utilizados também os Sistemas DMA e *Market* Datas, dentre outros, de senha individual para garantir a disponibilidade do sistema a seu usuário legítimo e seu uso por um único Colaborador, evitando que a conexão em uso seja desconectada.

A Vanquish utiliza o antivírus Kaspersky e monitoramento da rede e do tráfego de dados, além de controlar eventuais instalações de sistemas ou *softwares* não autorizados.

Os serviços de processamentos de dados e ou armazenamento em nuvem, *software* (SaaS) ou armazenamento de base de dados, através de interfaces HTTPS e autenticação segura, ocorrem em ambientes segregados.

11. Senhas

Os acessos ao ambiente tecnológico da Vanquish são controlados por meio de *logins* e senhas individuais, previamente autorizados, de acordo com a atividade de cada usuário colaborador ou administrador.

É fundamental que a senha seja criada pelo próprio colaborador, com caracteres alfanuméricos e com, no mínimo, seis dígitos.

O *login* e a senha são de uso pessoal e intransferível, dando acesso exclusivo ao Colaborador aos sistemas da Vanquish. Este vínculo garante que o respectivo *login* seja utilizado somente por um único colaborador.

12. Compartilhamento de incidentes

A Vanquish, caso venha a ocorrer incidentes relevantes que afetem seus sistemas críticos contratados e tenham impacto significativo sobre os clientes, os órgãos de administração e a SMI, deverá comunicar ao Diretor de Riscos e Compliance para medidas legais urgentes.

Caso ocorra algum incidente interno de segurança ou suspeitas, este deverá ser tempestivamente formalizado pelo Diretor Responsável pela Tecnologia e à empresa terceirizada responsável. Paralelamente, os colaboradores da Área de Tecnologia da Vanquish elaborarão documentação com cada etapa para detectar a criticidade do incidente, da utilização do *software* e *hardware* e trilha de auditoria, mantendo a confidencialidade e segurança física dos demais ambientes de operação e processamento.

13. Testes de Segurança

A fim de verificar a integridade dos sistemas adotados, inclusive com relação aos sistemas de informações confidenciais mantidas em meio eletrônico, a equipe de tecnologia da informação realiza testes periódicos e formaliza os resultados ao Diretor de Riscos, Compliance e PLD/FTP.

14. Atualizações

Esta Política está sujeita a revisões anuais, podendo ser revisada em periodicidade menor, em decorrência de alterações na regulamentação aplicável ou em alterações nos procedimentos internos.

15. Controle de Revisões

Política	Data	Motivo
Elaboração	Março/2023	Revisão por troca de controle acionário