MANUAL DE SEGURANÇA CIBERNÉTICA, SIGILO E SEGURANÇA DAS INFORMAÇÕES

17 de abril de 2023

CITREUS

ÍNDICE

1 Introdução

O manual de Segurança Cibernética, Sigilo e Segurança das Informações elaborado pela Citreus Serviços Fiduciários LTDA (Citreus), inscrita no CNPJ sob o nº 19.179.087/0001-34, visa delinear e especificar como tratamos das infromações que estão em nosso poder, bem como mecanismos e sistemas utilizados.

2 Escopo

O Escopo deste manual de Segurança Cibernética, Sigilo e Segurança das Informações é apresentar a metodologia aplicada na guarda de informações, sistemas, conduta e tratamento das informações seja por meios eletronicos ou vóz.

3 Abrangência

O escopo de atividade da Citreus se concentra na administração de fundos de investimento em participações (FIPs) e Fundo de Investimentos em Cotas (FICs), sendo assim, este manual foi elaborado dirigindo-se a este espectro dentro da ICVM 558 e Código ANBIMA de Regulação e Melhores Práticas de Administração de Recursos de Terceiros ("Código de ART").

4 Identificação de Pontos Relevantes de Atenção

Equipamentos de voz: A linha telefônica da Citreus é somente acessada in-loco, dentro de nosso escritório que para acessar é necessário cracha de acesso.

Comunicações eletrônicas: Utilizamos serviço de e-mail protegido por senha, criptografado e com as informações armazendas em nuvem, protegido de ataques externos.

Servidores: Utilizamos a salvaguarda de todas as informações da empresa na nuvem com back-up realizado em sistema de redudante em nuvem.

5 Potenciais Riscos

Perda de dados confidenciais: Perda de dados confidenciais, ou seja, informações sobre clientes, nossas carteiras, dados contábeis e comunicações

entre os colaboradores da Citreus e Clientes ou Cotistas.

Perda de dados operacionais: Perda de dados operacionais que resultem em perda de processamento da carteira de fundos, seu patrimônio líquido, calculo por cotista e aspectos contábeis do fundo.

Impossibilidade de acesso à informações: Falhas em harware, softwares e provedores de sistemas que impossibilitem o acesso à informações e atrapalhem a operação da Citreus.

6 Tipos de Ameaças

Ameaças internas: uso de informações internas de maneira intencional ou não intencional.

Ameaças externas: perda da integridade das informações que estão em posse da Citreus realizada por terceiros.

7 Salvaguarda das informações: aspectos de proteção

Manuais de Conduta: O nosso Manual de Compliance e Ética e Código de Ética, é de leitura obrigatória a todos os colaboradores e objeto de treinamento periódico. Nele há estipulado as penalidades que colaboradores que "vazam" informações podem sofrer.

Controle de informações USB: Somente disponível aos Sócio-Diretores da Empresa.

Instalação de Softwares: Somente permitida a instalação de Softwares pelos Sócio-Diretores da Citreus.

Acesso às Informações: Toda e qualquer informação sigilosa somente é acessada por senha em diferentes níveis e concessões de acordo com a atividade de cada colaborador.

Acesso remoto: Realizado somente pelos sócios-diretores da empresa e em ambiente controlado como sistemas operacionais da empresa com acesso via senha.

Antivirus e dispositivo de segurança de rede: Além dos acessos serem controlados, a Citreus também utiliza firewall e antivirus para proteção dos dados.

Aceso às informações: o acesso às informações são controlados e liberados de acordo com area de atuação de cada colaborador.

Salientamos, também, que qualquer sistema da Citreus é controlado e pode ser bloqueado instantâneamente em caso de ameaças ou suspeitas de mal uso de suas informações.

8 Supervisão de sistemas

Backup: As informações vitais da empresa, salvaguarda de arquivos importantes, informações de nosso sistema operacional e e-mail contam com processo de back-up periódico.

Controles Sistêmicos: Ainda, nossos sistemas possuem dispositivos que detectam ameaças externas para garantir a proteção de nossas informações.

9 Reação em casos de ameaças

Ameaças Externas: Imediatamente é acionado o responsável por tecnologia o qual deverá imediatamente atuar a fim de impedir que a ameaça permaneça e proteger a integridade dos sistemas da Citreus e suas informações. Nestes casos há a possibilidade da retirada dos sistemas em operação, restauração dos mesmos e utilização de seus back-ups em nuvem.

Ameaças Internas: O Diretor de Compliance e risco é acionado para instaurar sindicancia em relação ao colaborador que teve este grave desvio de conduta. Após apuração do ocorrido as medidas cabiveis, estipuladas na lei e em nosso Código de Ética e Manual de Compliance serão aplicadas.

10 Responsável pela área de Compliance e Risco

O responsável pela Área de Compliance e risco é o Sr. Tijs Willem Jansen, sendo o responsável pela aplicação deste Manual, tratamento da segurança Cibernética, Sigilo e Segurança das Informações.

Versão	Data	Aprovado	Responsável
1	17/4/23	Aprovado	Tijs Jansen