Canepa
Asset Brasil

Política de Segurança Cibernética

Dezembro 2018

Versão atual: dezembro/2018
Versão anterior: N/A

Canepa
Asset Brasil

Versão atual: dezembro/2018
Versão anterior: N/A

1. INTRODUÇÃO

A presente Política de Segurança Cibernética ("Política") elenca os principais aspectos de cibersegurança adotados pela Canepa Asset Management - Cam Brasil Gestão de Recursos Ltda. ("**Canepa**") com o objetivo de lidar com possíveis ameaças cibernéticas.

Os colaboradores atestam a ciência e adesão acerca dos procedimentos definidos pela presente Política mediante assinatura de termo próprio, sendo submetidos anualmente ao Programa de Treinamento adotado pela Sociedade, a fim de que sejam orientados sobre as rotinas a serem observadas no desempenho dos processos descritos nesta Política.

A fim de cumprir o seu objetivo, esta Política será revisada no mínimo a cada 2 (dois) anos, sendo mantido o controle de versões, e circulada aos colaboradores para conhecimento sempre que sofer alterações.

Em caso de dúvidas ou necessidade de aconselhamento, o colaborador deve buscar auxílio junto ao Diretor de Compliance da **Canepa**, devendo as questões de segurança cibernética serem tratadas com o responsável pela área de Tecnologia da Informação da **Canepa**.

2. CONCEITO

A Segurança Cibernética é composta pelos seguintes pilares:

- Confidencialidade: O acesso à informação deve ser restrito apenas às pessoas autorizadas pela direção da **Canepa**.

- Integridade: Somente alterações, supressões e adições autorizadas pela **Canepa** podem ser realizadas nas informações.

- Disponibilidade: Sempre que necessário ou demandado, a informação deve estar disponível para as pessoas autorizadas.

Para assegurar esses três itens mencionados, a informação deve ser adequadamente gerenciada e protegida contra roubo, fraude, espionagem, perda não-intencional, acidentes e outras ameaças.

A presente Política, em conjunto com a Política de Segurança da Informação adotada pela **Canepa**, em manual próprio, preconiza a informação como bem da **Canepa** e exige de todos os colaboradores o zelo pela sua confidencialidade, especialmente as informações relativas aos seus clientes/investidores (informações cadastrais, bancárias, financeiras, informações relativas às preferências de investimentos, dentre outras).

3. AVALIAÇÃO DE RISCOS

A avaliação dos riscos, bem como a identificação dos ativos e suas vulnerabilidades é realizado para Área de Compliance em conjunto com a empresa contratada para suporte ao parque tecnólogica da **Canepa**.

Considerando a atividade de gestão profissional de recursos de terceiros desempenhada pela **Canepa** são essenciais todos os recursos tecnológicos necessários ao processo de análise, investimento e desinvestimento, tais como: (i) disponibilização das informações diárias sobre os fundos sob gestão; (ii) boletagem de operações; (iii) compra e venda de ativos para as carteiras sob gestão; (iv) conferência e liberação das carteiras diárias dos fundos sob gestão; e (v) acesso aos sistemas de informação, inclusive aqueles relacionados ao cliente. Alguns exemplos:

- LOTE45
- Broadcast
- Bloomberg
- SMA (Sistema BNY Mellon de Atendimento)

Diante da possibilidade de invasores utilizarem (i) Malware, (ii) Engenharia social; (iii) Pharming; (iv) Phishing; (v) Vishing; (vi) Smishing; (vii) Acesso pessoal; (viii) Ataques de DDos (distributed denial of services) e botnets; e (ix)

Invasões (advanced persistent threats, a Sociedade adota ações de prevenção e proteção, nos termos do Capítulo seguinte.

4. PROTEÇÃO E PREVENÇÃO

Os planos de ação e prevenção descritos neste capítulo da Política têm por objetivo mitigar e minimizar a possibilidade de ocorrência de um ataque cibernético, na tentativa de evitar que os riscos identificados se concretizem.

Neste sentido, a **Canepa** ratifica a adoção de controles de acesso físico e lógico implementados em linha com a Política de Segurança da Informação adotada. Tais controles visam a identificação, autenticação e autorização de acesso pelos usuários a sistemas ou ativos da **Canepa**, evitando o acesso por terceiros não autorizados.

Isto posto, todos os colaboradores devem observar de forma estrita as rotinas relacionadas à definição de senhas de acesso aos sistemas e rede, bem como às barreiras da informação com relação a outras atividades desempenhadas pela **Canepa** ou empresas do mesmo grupo econômico.

Os eventos de login e alteração de senhas são rastreáveis e auditáveis, sendo qualquer inconsistência ou inadequação com relação aos acessos recomendados pelo Diretor de Compliance reportados imediatamente. Especial atenção deverá ser envidada aos casos de desligamento ou gozo de férias de colaboradores.

São adotadas as seguintes medidas preventivas para cada risco identificado:

- Os principais servidores, que contemplam os arquivos estão em uma rede protegida por um Appliance PFSENSE (Firewall) com Controle de IDS (Intrusion detection system) e DDoS, Antivírus com regras específicas para acesso, bloqueando quaisquer conexões não autorizadas.

- Acesso VPN com controle de acesso administrado pelo Active Directory e software cliente com criptografia OpenVPN.

- Todas as estações de trabalho e servidores possuem, instalados e atualizados diariamente, o sistema antivírus TREND, no qual existem regras que bloqueiam potenciais sites que possam trazer qualquer tipo de ameaça (Pharming, Phishing), assim como, total proteção a ransomwares, Malwares, Vírus, Cavalo de troia, Spywares e Engenharia Social, além de constante comunicação para que os usuários não abram links nos quais não saibam a procedência.

5. SUPERVISÃO

São realizados os testes de verificação para fins de identificação de anomalias, detecção de ameaças, acessos, componentes ou dispositivos não autorizados. A detecção automática de falhas em servidor de monitoramento (NAGIOS e ZABBIX) permite a prevenção de indisponibilidade em todos os hardwares (servidores), software e links (Broadcast, Bloomberg, internet, site e etc).

São mantidos inventários atualizados de hardware e softwares utilizados. Anualmente são realizadas verificações, a fim de identificar elementos estranhos, tais como computadores não autorizados ou softwares não licenciados.

Sempre que houver alteração relevante na estrutura tecnológica da **Canepa** serão realizadas análises de vulnerabilidade.

6. PLANO DE CONTINUIDADE DE NEGÓCIOS

A **Canepa** dispõe de um plano de respostas a incidentes tratado em manual próprio e contempla diversos cenários de ameaça a continuidade de seus negócios, nos termos do Plano de Continuidade de Negócios adotado internamente.

7. RESPONSABILIDADE

O responsável por questões de cibersegurança é o Diretor de Compliance com o apoio de empresa terceirizada.

8. PROGRAMA DE TREINAMENTO

A **Canepa** conta com um Programa de Treinamento, detalhadamente descrito no Código de Ética e Conduta, dos colaboradores que tenham acesso a informações relevantes sobre a instituição, seus negócios ou clientes/investidores.

Os procedimentos e rotinas definidos na presente Política serão abordados em treinamento anual, coordenado pelo Diretor de Compliance ou terceiro contratado para esta finalidade, visando a sua disseminação entre a equipe.

Poderão ser promovidos treinamentos em periodicidade menor, visando a atualização e ampliação do conhecimento dos colaboradores, em especial em virtude de mudanças relevantes nos procedimentos e controles descritos nesta Política.

9. DISPOSIÇÕES GERAIS E ENFORCEMENT

Todos os documentos, relatórios e informações relevantes para os procedimentos e rotinas descritos nesta Política são arquivados em meio físico ou eletrônico na **Canepa**, pelo prazo mínimo de 5 (cinco) anos.