POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E SEGURANÇA CIBERNÉTICA

APOLO ADMINISTRAÇÃO DE RECURSOS LTDA

Março/2021

Sumário

OBJETIVOS 3
SEGURANÇA DA INFORMAÇÃO 3
SEGURANÇA CIBERNÉTICA 5
TREINAMENTO DE SEGURANÇA DAS INFORMAÇÕES 6
RELATÓRIO DE TESTES DE SEGURANÇA CIBERNÉTICA 6
VIGÊNCIA E ATUALIZAÇÃO 7

APRESENTAÇÃO

A Política de Segurança da Informação da Apolo Administração De Recursos Ltda.(“Apolo

Asset"), aplica-se a todos os sócios, colaboradores, prestadores de serviços, incluindo trabalhos executados externamente ou remotamente ou por terceiros que utilizem o ambiente de sistemas de processamento da Apolo, ou que acessem informações a esta pertencentes. Todo e qualquer usuário de recursos computadorizados, digitais ou sistêmicos da Apolo tem a responsabilidade de proteger a segurança e a integridade das informações e dos equipamentos de informática.

OBJETIVOS

A Política de Segurança da Informação da Apolo visa proteger as informações de sua propriedade e/ou de terceiros que estejam sob sua guarda, garantindo a disponibilidade, integridade, confidencialidade, legalidade, autenticidade e auditabilidade das mesmas.

Sendo assim, nenhuma informação confidencial deve, em qualquer hipótese, ser divulgada a pessoas, dentro ou fora da Apolo Asset, que não necessitem de, ou não devam ter acesso a tais informações para desempenho de suas atividades profissionais relacionadas à empresa.

Qualquer informação sobre a Apolo Asset, ou de qualquer natureza relativa às atividades da empresa e a seus sócios, colaboradores e clientes, obtida em decorrência do desempenho das atividades normais de qualquer colaborador, só poderá ser fornecida ao público, mídia ou a demais órgãos caso autorizado pelo Diretor de Riscos e *Compliance* ou se permitido de qualquer forma pela presente política.

SEGURANÇA DA INFORMAÇÃO

As medidas de segurança da informação utilizadas pela Apolo Asset têm por finalidade minimizar as ameaças ao patrimônio, à imagem e aos negócios da empresa e aos seus clientes.

É terminantemente proibido aos Colaboradores fazerem cópias ou imprimir os arquivos utilizados, gerados ou disponíveis da Apolo Asset para circulação em ambientes externos à empresa, sem a prévia e expressa autorização do Diretor de Riscos e *Compliance*. Isso porque tais arquivos contêm informações que são consideradas informações confidenciais e/ou sensíveis aos objetivos sociais da Apolo Asset. Cabe ressaltar que, em relação às informações de caráter sensível ou confidencial da empresa ou de clientes, estas serão armazenados em diretórios de rede, com *back up* em nuvem e acesso restrito, e controlado pela equipe de Riscos e *Compliance* da Apolo Asset.

A proibição acima referida não se aplica quando as cópias ou a impressão dos arquivos forem

comprovadamente em prol da execução e do desenvolvimento dos negócios e dos interesses da Apolo Asset. Nestes casos, o colaborador que estiver na posse e guarda da cópia ou da impressão do arquivo que contenha a informação confidencial será o responsável direto por sua boa conservação, integridade e manutenção de sua confidencialidade, responsabilizando-se também por seu extravio ou uso indevido. Ainda, qualquer impressão de documentos deve serprontamente retirada da máquina impressora, pois podem conter informações restritas econfidenciais, mesmo no ambiente interno da Apolo Asset, e a depender do conteúdo do documento, deverá ser feita a reserva da impressora para que outros não a utilizem simultaneamente

O descarte de informações confidenciais em meio digital deve ser feito de forma a impossibilitar sua recuperação. O descarte de documentos físicos que contenham informações confidenciais ou de suas cópias deverá ser realizado imediatamente após seu uso, de maneira a evitar sua recuperação, sendo recomendável o seu descarte total, preferencialmente utilizando máquina trituradora de papel.

Adicionalmente, os colaboradores devem se abster de utilizar pen-drives, disquetes, fitas, discosde hard drive ou quaisquer outros meios que não tenham por finalidade a utilização exclusiva para o desempenho de sua atividade na Apolo Asset.

É proibida a conexão de equipamentos na rede da Apolo Asset que não estejam previamente autorizados pelo Diretor de Riscos e *Compliance* ou pelo responsável pela TI. Novos equipamentos e/ou sistemas deverão ter suas configurações realizadas em ambientes de homologação. Ao menos dois equipamentos serão mantidos prontos e configurados para utilização em caráter de back-up, caso haja necessidade por motivo de problemas nos equipamentos em uso.

Cada colaborador é responsável por manter o controle sobre a segurança das informações armazenadas ou disponibilizadas nos equipamentos que estão sob sua responsabilidade. Será obrigatória a alteração de senha de acesso aos equipamentos (login de usuário) ao menos a cadadois meses, utilizando modelo de definição de senha de difícil identificação por parte depotenciais "hackers" externos. Tal processo será auditável e rastreável eletronicamente pelo responsável pela TI, sob a supervisão do Diretor de Riscos e *Compliance* da Apolo Asset**.**

O acesso a sites e blogs, bem como o envio ou repasse por e-mail de material que contenha conteúdo discriminatório, preconceituoso, obsceno, pornográfico, de cunho político ou de

qualquer forma ofensivo também é terminantemente proibido, como também o envio ou repasse de e-mails com opiniões, comentários ou mensagens que possam denegrir a imagem eafetar a reputação da Apolo Asset, respondendo os responsáveis nos termos das políticas internas da Apolo Asset e da lei.

Programas instalados nos computadores, principalmente via internet (downloads), sejam de utilização profissional ou para fins pessoais, devem obter autorização prévia dos sócios, além de avaliação de segurança pela empresa contratada para prover suporte de TI. Não é permitida a instalação de nenhum software ilegal ou que possuam direitos autorais protegidos, ou mesmo legal, sem prévia autorização do Diretor de Riscos e *Compliance*.

Os colaboradores ou prestadores de serviços desligados da Apolo Asset terão os seus acessos aos sistemas e programas de propriedade da Empresa ou adquiridos de terceiros imediatamente bloqueados após a comunicação de desligamento de tais colaboradores ou prestadores de serviços, de forma a preservar as informações confidenciais, reservadas ou privilegiadas.

Todo conteúdo que está na rede pode ser acessado pelos sócios ou pelo Diretor de Riscos e *Compliance* caso haja necessidade, inclusive e-mails. Arquivos pessoais salvos em cada computador poderão ser acessados, caso seja necessário. A confidencialidade dessasinformações deve ser respeitada, e seu conteúdo será disponibilizado ou divulgado somente nostermos e para os devidos fins legais, ou em atendimento a determinações judiciais ou administrativas.

Por fim, convém ressaltar que a Apolo Asset conta com sistemas e ferramentas contratados para arquivamento, firewall, antivírus, backup, e linha de contingência.

SEGURANÇA CIBERNÉTICA

Identificação e Avaliação de Riscos

Existem muitos motivos para que ataques sejam feitos pelos mais variados agentes (organizações criminosas ou hackers, organismos de Estado, terroristas, colaboradores, competidores, etc.). Os principais motivos identificados são:

i) Obter ganho financeiro;
ii) Roubar, manipular ou adulterar informações;
iii) Obter vantagens competitivas e informações confidenciais de empresas

concorrentes;

iv) Fraudar, sabotar ou expor a instituição invadida, podendo ter como motivo acessório a vingança;

v) Promover ideias políticas e/ou sociais; e

vi) Praticar o terror e disseminar pânico e caos.

A Apolo Asset deverá identificar e avaliar os principais riscos cibernéticos aos quais está exposta. O Código ANBIMA de Segurança Cibernética definiu que os ataques mais comuns de criminosos cibernéticos são os seguintes:

a) Malware (Vírus, Cavalo de Troia, Spyware e Ransomware);
b) Engenharia Social (Pharming, Phishing, Vishing, Smishing e Acesso Pessoal);
c) Ataques de DDoS (Distributed denial of services) e botnets; e
d) Invasões (advanced persistent threats).

TREINAMENTO DE SEGURANÇA DAS INFORMAÇÕES

A Apolo Asset entende essencial que o seu treinamento anual, supervisionado pelo Diretor de Riscos e *Compliance e* pela empresa de suporte de TI, abranja todos os preceitos contidos na presente política, de modo que seus, sócios e colaboradores e profissionais que tenham acesso a informações confidenciais, reservadas ou privilegiadas e estejam sempre cientes e consonantes aos procedimentos de proteção, segregação e segurança das informações.

RELATÓRIO DE TESTES DE SEGURANÇA CIBERNÉTICA

Mensalmente, a Apolo Asset realizará testes dos seus sistemas de segurança de informações, sobretudo aquelas em meio eletrônico, bem como de todos os preceitos contidos na presente política, incluindo, mas não se limitando aos procedimentos de descarte de informações pelos colaboradores, individualização dos usuários.

Todos os resultados desses testes, bem como os procedimentos para saneamento de eventuais problemas, serão descritos no Relatório Anual de Controles Internos da Apolo Asset que será arquivado na sede da Apolo Asset sob a responsabilidade do Diretor de Riscos e *Compliance*.

Os testes serão realizados pela equipe de suporte de TI contratada, e buscarão cobrir os seguintes pontos:

- Identificação e avaliação de potenciais riscos cibernéticos, envolvendo ativos de hardware e software, além de processos que necessitem de proteção. Importante estimar impactos financeiros, operacionais e reputacionais em caso de evento;
- Criação de um plano de resposta a incidentes, considerando os cenários de ameaças previstos durante a avaliação de riscos, que permita a continuidade dos negócios ou a recuperação adequada em casos mais graves;
- Estabelecimento de medidas de prevenção e mitigação de riscos identificados na atividade de identificação de riscos, de forma a buscar evitar eventuais ataques cibernéticos aos dados e equipamentos da empresa;
- Detecção de possíveis anomalias e/ ou fragilidades no ambiente tecnológico, incluindo acessos não permitidos, usuários não cadastrados, e dispositivos não autorizados;
- Criação de um plano de resposta e recuperação de incidentes, considerando cenários de ameaças previstas durante a avaliação de riscos que contenha comunicação interna e externa, e que permita a continuidade dos negócios ou a recuperação adequada em casos mais graves. Tal plano será elaborado em conjunto entre as áreas internas de Riscos e *Compliance*, e da empresa de TI contratada. O plano identificará papéis e responsabilidades, com previsão de acionamento de colaboradores e contatos externos;
- Manutenção do programa de segurança cibernética atualizado;
- Identificação de vazamentos de informações confidenciais, reservadas ou privilegiadas e o procedimento específico a ser adotado em tais circunstâncias (colocar de uma forma que não somos responsáveis por identificar)

As documentações relacionadas aos planos definidos e testes realizados, assim como os resultados auferidos e ações corretivas e mitigantes, deverão ser mantidas em diretório interno da área de Riscos e *Compliance* como evidência em eventuais questionamentos internos ou de órgãos reguladores ou autorreguladores.

Os temas relacionados à segurança da informação e cibernética serão tratados no Comitê de Riscos e *Compliance*, de forma ordinária, ou mesmo em reunião específica, em casos de eventos extraordinários, para que sejam tomadas de forma tempestiva medidas de recuperação, limitação de danos, e resposta relevante.

VIGÊNCIA E ATUALIZAÇÃO

Esta Política será revisada anualmente, e sua alteração acontecerá caso seja constatada

necessidade de atualização do seu conteúdo. Poderá, ainda, ser alterada a qualquer tempo emrazão de circunstâncias que demandem tal providência.

A Presente Política está atualizada e em conformidade com a Lei Geral de Proteção de Dados, Lei Federal 13.709/19.

Histórico das Atualizações		
Data	Versão	Responsável
Maio de 2021	1ª e Atual	Diretor de Compliance e Risco