Política para Segurança Cibernética

Eagle Capital

Elaboração: Janeiro de 2021

Atualização: Junho 2023

Sumário

1. Finalidade

A finalidade da presente Política para Segurança Cibernética ("Política") é a de estabelecer padrões mínimos para a zelar pela segurança de seus negócios, registros e informações contra riscos e, também, ataques cibernéticos que podem ocorrer à Eagle Capital Gestão de Investimentos Ltda ("Eagle Capital").

2. Abrangência

Esta Política aplica-se a todos sócios, funcionários, estagiários ("Colaboradores") da Eagle Capital, bem como de suas coligadas e controladas se e quando constituídas, e abrange todas as atividades da empresa incluindo todas as atividades que possam ou venham a ser terceirizadas.

Todos os nossos colaboradores têm a responsabilidade de proteger a segurança e integridade de nossos arquivos contra vazamento de informações, ameaças cibernéticas e acessos não-autorizados, e para tanto, encontram-se alinhados às melhores práticas de cibersegurança e segurança da informação.

3. Programa para Segurança Cibernética

As ameaças cibernéticas podem variar, ainda, em função da natureza, vulnerabilidade e informações/bens de cada organização. Os invasores podem valer-se de vários métodos para a r ealização de um ataque cibernético. Os mais comuns são:

- Malware (vírus, cavalo de tróia, spyware, etc);
- Engenharia social (pharming, phishing, vishing, entre outros);
- 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 um grande número de computadores utilizados para criar e mandar spam ou vírus, ou inundar uma rede com mensagens resultando na negação de serviços.

- Invasões (advanced persistent threats) – ataques realizados por invasores sofisticados, utilizando conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico.

4. Ações de Prevenção e Medidas de Proteção

- Visando mitigar e minimizar a concretização dos riscos identificados, a Eagle Capital adota medidas que busquem impedir previamente a ocorrência de um ataque cibernético, como:
- Controle do acesso aos ativos da Gestora, por meio de identificação, autenticação e autorização dos usuários ou sistemas;
- Estabelecimento de regras mínimas na definição de senhas de acesso a dispositivos corporativos, sistemas e rede - complexidade, periodicidade e autenticação de múltiplos fatores - em função da relevância do ativo acessado;
- Segregação de senhas entre serviços;
- Limitação do acesso, uma vez concedido, a apenas recursos relevantes para o desempenho das atividades. A concessão de acesso será implementada de forma a ser revogada rapidamente quando necessário;
- Os eventos de login e alteração de senhas na Eagle Capital serão auditáveis e rastreáveis;
- Ao incluir novos equipamentos e sistemas em produção, a Eagle Capital garantirá que serão feitas configurações seguras de seus recursos;

- Restrição ao acesso físico às áreas com informações críticas/sensíveis;

- Criação de logs e trilhas de auditoria sempre que os sistemas permitirem;

- Realização de diligência na contratação de serviços de terceiros, inclusive serviços em nuvem, com adequação a questões jurídicas, incluindo cláusulas de confidencialidade, proteção de dados pessoais e exigência de controles de segurança na própria estrutura dos terceiros;

- Implementação de segurança de borda, nas redes de computadores, por meio de firewalls e outros mecanismos de filtros de pacotes;

- Implementação de recursos anti-malware em estações e servidores de rede, como antivírus e firewalls pessoais;

- Implementação de segregação de serviços sempre que possível, restringindo-se o tráfego de dados apenas entre os equipamentos relevantes;

- Impedimento à instalação e execução de software e aplicações não autorizadas por meio de controles de execução de processos (por exemplo, aplicação de whitelisting); e

- Todas as informações do servidor da Eagle Capital devem ser armazenados e manter back up remoto.

5. Monitoramento

Conforme recomendado pela Anbima, a Eagle Capital faz uso de mecanismos para monitoração de seus sistemas. A seguir, estão elencadas algumas das medidas tomadas:

- Criação de mecanismos de monitoramento de todas as ações de proteção implementadas para garantir seu bom funcionamento e efetividade;

- Manutenção de inventários atualizados de hardware e software, bem como verificação destes com frequência para identificar elementos estranhos à instituição;

- Manutenção dos sistemas operacionais e softwares de aplicação sempre atualizados, instalando as atualizações sempre que forem disponibilizadas;

- Monitoramento diário das rotinas de backup; e

- Realização de análises de vulnerabilidades na estrutura tecnológica, periodicamente ou sempre que houver mudança significativa em tal estrutura.

6. Vigência e Revisão da Política

Esta Política entra em vigor na data de sua publicação conforme consta na primeira página da política e deverá ser revisada anualmente pela Área de Compliance da Eagle Capital, bem quando for publicada leis, normas ou circulares que impactem de alguma forma esta Política.