POLÍTICA DE SEGURANÇA CIBERNÉTICA

BLUE STAR ASSET E MANAGEMENT LTDA.
CNPJ/MF 10.757.089/0001-99
NIRE 35223119864

Estas Políticas de Segurança Cibernética e de Segurança das Informações da **BLUE STAR ASSET E MANAGEMENT LTDA.** ("Políticas", ou individualmente, "Política"), sociedade limitada com seu contrato social devidamente arquivado na Junta Comercial do Estado de São Paulo - JUCESP sob o NIRE 35.223.119.864, inscrita no CNPJ/MF sob o nº 10.757.089/0001-99, com sede na Cidade de São Paulo, Estado de São Paulo, na Rua Helena, nº 285, conjunto 112, Vila Olímpia, CEP 04552-050 ("Sociedade" ou "Blue Star") encontram-se sob a responsabilidade de sua respectiva Diretoria de *Compliance*.

POLÍTICA DE SEGURANÇA CIBERNÉTICA

A presente Política de Segurança Cibernética, dispõe acerca das regras e procedimentos para o programa de segurança cibernética visando mitigar o risco de ataques cibernéticos à companhia.

O Programa

A Sociedade estruturou um programa baseado em cinco principais funções contra ataques cibernéticos. O programa foi desenhado em conjunto entre a empresa de tecnologia de informação que presta serviços para a Blue Star e os gestores de risco e Compliance e de ativos da companhia. Seguem as principais funções, assim como um detalhamento do programa:

(i) **Identificação/avaliação de riscos (risk assessment):** identificar os riscos internos e externos, os ativos de hardware e software e processos que precisam de proteção.

- Todos os acessos externos são bloqueados por um roteador central.
- As estações de trabalho não permitem acessos remotos sem autorização da equipe técnica
- Todas as estações de trabalho possuem softwares homologados e atualizados.

- Atualizações periódicas são aplicadas automaticamente e monitoradas pela equipe técnica.

(ii) **Ações de prevenção e proteção:** estabelecer um conjunto de medidas cujo objetivo é mitigar e minimizar a concretização dos riscos identificados no item anterior, ou seja, buscar impedir previamente a ocorrência de um ataque cibernético, incluindo a programação e implementação de controles.

- Arquivos e documentos oficiais são armazenados em nuvem com autenticações em dois fatores (2FA).
- Arquivos com informações confidenciais e de alto nível de acesso são criptografados.
- As senhas definidas pela empresa possuem requisitos mínimos, como: mínimo de 10 caracteres, letras maiúsculas e minúsculas, além de números e caracteres especiais.
- Acessos de equipes externas (como profissionais de propaganda, equipes de business intelligence ou TI) são refeitos e possuem efeito temporário para determinada atividade.
- Todas as alterações ou tentativa de acesso externo possui rastreabilidade por parte da equipe de TI.

(iii) **Monitoramento e testes:** detectar as ameaças em tempo hábil, reforçando os controles, caso necessário, e identificar possíveis anomalias no ambiente tecnológico, incluindo a presença de usuários, componentes ou dispositivos não autorizados.

- Atualizações periódicas do Sistemas Operacionais e programas.
- Realização de backup automático de todos os sistemas.
- Atualização de hardware defasado.

(iv) **Criação do plano de resposta:** ter um plano de resposta, tratamento e recuperação de incidentes, incluindo um plano de comunicação interna e externa, caso necessário.

- Contato direto com equipe técnica em caso de crise ou vulnerabilidade do sistema.
- Atendimento prioritário pela equipe de Cloud Service e Armazenamento em nuvem.
- Ações de urgência podem ser resolvidos mesmo de forma externa.
- Adaptação de crises atuais para cenários futuros.

(v) **Reciclagem e revisão:** manter o programa de segurança cibernética continua e/ou anualmente atualizado, conforme aplicável, identificando novos riscos, ativos e processos e reavaliando os riscos residuais.

- Acompanhamento periódico com as equipes e estações de trabalho para manter os sistemas atualizados.
- Inscrição de grupos internos em palestras sobre tendências tecnológicas e segurança digital.
- Orientação para conservação e manutenção de equipamentos.
- Troca e manutenção sustentável dos equipamentos visando não somente a performance da equipe, mas também descarte/troca consciente.

Considerações Finais

A Blue Star entende a relevância do assunto tratado pelo programa e criou essa política visando mitigar ao máximo o risco de um ataque cibernético. Uma rápida detecção e resposta são essenciais para evitar um impacto sobre a companhia e seus clientes, no caso de um eventual problema. Para tal, sempre há a supervisão de um dos sócios da companhia no acompanhamento do processo.

São Paulo, 12 de fevereiro de 2019.

* * *