LIS CAPITAL

POLÍTICA DE CONTINUIDADE E SEGURANÇA CIBERNÉTICA

LIS CAPITAL - ADMINISTRADORA E GESTORA DE RECURSOS FINANCEIROS LTDA.

Escopo	Área de Compliance, Risco e PLDFT
Autor	Tito Ávila _ Diretor de Risco e Compliance
Próxima Revisão	janeiro-23

Versão	Data	Supervisão
1	janeiro-21	Tito Ávila _ Diretor de Risco e Compliance
2	janeiro-22	Tito Ávila _ Diretor de Risco e Compliance

1. ASPECTOS GERAIS

Esta política deve ser interpretada conjuntamente com as demais políticas internas da LIS Capital e com asleis e normas vigentes.

Todos devem se assegurar do perfeito entendimento das leis e normas aplicáveis à LIS Capital, bem comodo completo conteúdo desta política e das demais políticas internas da LIS Capital. Em caso de dúvidas ou necessidade de aconselhamento, é imprescindível que se busque auxílio imediato junto ao departamento deCompliance.

2. OBJETIVO

O presente POLÍTICA DE CONTINUIDADE E SEGURANÇA CIBERNÉTICA tem como objetivo estabelecer práticas da LIS CAPITAL – ADMINISTRADORA E GESTORA DE RECURSOS FINANCEIROS LTDA ("LIS Capital") aderente ao Código ANBIMA de Regulação e Melhores Práticas para Administração de Recursos de Terceiros e suas respectivas diretrizes e deliberações.

Essa POLÍTICA DE CONTINUIDADE E SEGURANÇA CIBERNÉTICA foi elaborado seguindo o Guia de Cibersegurança ANBIMA para atender especificamente às atividades desempenhadas pela LIS Capital, de acordo com natureza, complexidade e riscos a elas inerentes, observada a obrigação de revisão e atualização periódica. A LIS Capital contrata a empresa TECNOQUALIFY CONSULTORIA E COMERCIO LTDA. para o fornecimento de sua infraestrutura de tecnologia da informação.

O objetivo das regras sobre segurança da informação da LIS Capital é primordialmente assegurar a proteçãode seus ativos de informação contra ameaças, internas ou externas, reduzir a exposição a perdas ou danos decorrentes de falhas de Cibersegurança e garantir que os recursos adequados estarão disponíveis, mantendo um programa de segurança efetivo e conscientizando seus Colaboradores a respeito.

3. APLICABILIDADE

A efetividade desta Política depende da conscientização de todos os Colaboradores e do esforço constantepara que seja feito bom uso das Informações Sigilosas e dos Ativos disponibilizados pela LIS Capital ao Colaborador.

Esta Política deve ser conhecida e obedecida por todos os Colaboradores que utilizam os recursos de tecnologia disponibilizados pela LIS Capital, sendo de responsabilidade individual e coletiva o seu cumprimento. A LIS Capital apresenta uma abordagem holística em relação à segurança cibernética, sendo obrigação do Diretor Riscos, Compliance & PLDFT, Tito Ávila, promover treinamentos para que os Colaboradores saibam as suas respectivas funções na proteção de Informações Sigilosas, para que possam agir de maneira apropriada frente as situações que requeiram respostas.

4. PROCESSO

Os processos de segurança de dados e da informação da LIS Capital devem assegurar:

- A integridade (garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais);
- A disponibilidade (garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário);
- A confidencialidade dos ativos de informação (garantia de que o acesso à informação seja obtido somente por pessoas autorizadas) da LIS Capital, observadas as regras de confidencialidade constantes do Código de Ética da LIS Capital; e
- O confinamento das informações confidenciais dentro do perímetro de segurança digital designadono tópico subsequente.

5. CONCEITO

Todas as Informações Sigilosas constituem ativos de valor para a LIS Capital, e, por conseguinte, precisam ser adequadamente protegidas contra ameaças e ações que possam causar danos e prejuízos para a LIS Capital, Clientes, Fundos e Colaboradores.

As Informações Sigilosas podem ser armazenadas e transmitidas de diversas maneiras, como, por exemplo,arquivos eletrônicos, mensagens eletrônicas, sites de Internet, bancos de dados, meio impresso, mídias de áudio e de vídeo, dentre outras. Cada uma dessas maneiras está sujeita a uma ou mais formas demanipulação, alteração, remoção e eliminação do seu conteúdo.

A adoção de políticas e procedimentos que visem a garantir a segurança de Informações Sigilosas deve serprioridade constante da LIS Capital, reduzindo-se os riscos de falhas, os danos e prejuízos que possam comprometer a imagem e os objetivos da LIS Capital.

O programa de Segurança Cibernética da LIS possui cinco pilares fundamentais:

- Identificação e Avaliação de Riscos (risk assessment);
- Recursos Relevantes;
- Ações de prevenção e proteção;
- Monitoramento e testes; e
- Plano de resposta.

6. SEGURANÇA CIBERNÉTICA

6.1 AVALIAÇÃO DE RISCOS (RISK ASSESSMENT)

Os principais riscos identificados pela LIS Capital como ameaças cibernéticas são:

- Acesso indevido a pastas, documentos internos, restritos e/ou sigilosos;
- Acesso indevido a informações de clientes e/ou potenciais clientes;
- Acesso indevido a propriedade intelectual, metodologias e planos de negócios;
- Acesso indevido a lista de usuários e quebra de senhas de sistemas;
- Manipulação e/ou adulteração de informações;
- Sabotagem com a finalidade de corromper e/ou tornar indisponível totalmente ou parcialmente oambiente de tecnologia.

- Ataques mais comuns de criminosos cibernéticos, definidos pelo Código ANBIMA: Malware (e.g.vírus, cavalo de troia, spyware e ransomware), Engenharia Social, Pharming, Phishing scam, Vishing, Smishing, Acesso pessoal, Ataques de DDoS e botnets; Invasões (advanced persistentthreats).

6.2 RECURSOS RELEVANTES

Abaixo estão listados os recursos relevantes da LIS Capital utilizados no processo de prevenção e SegurançaCibernética:

- Armazenamento de arquivos em nuvem (cloud computing);
- Versionamento e retenção de arquivos (histórico de versões de arquivos em nuvem);
- Anti-Virus AVG;
- Firewall;
- Switch TP-Link TL-SG 1024/24;
- Switchs nas mesas de trabalho para distribuição de rede cabeada;
- Controles de Acesso a Informações (Dropbox for Businesses);
- Controles de Acesso às dependências da LIS (Digital);
- No-Breaks APC;
- PABX Intelbras;
- Estações de trabalho na plataforma Windows 10 Pro;
- Google Inc. (Google Drive for Work), G Suite;
- Dropbox for Businesses;
- Serviço Telefônico e de Internet - Claro S.A; Serviço de Internet Backup – Dialdata Telecomunicações Ltda. (Evo Telecom).

6.3 AÇÕES DE PREVENÇÃO E PROTEÇÃO

Abaixo a LIS Capital lista ações de prevenção e proteção mapeadas à ataques cibernéticos:

- O Firewall está devidamente funcional e com os sistemas de proteção de borda ativos;
- Back-up diário completo e automático de todos os drives e arquivos da rede via cloud computing;
- Servidores e estações de trabalho atualizados com as últimas versões do fabricante;
- Equipamentos com antivírus ativo, integrado com o software de gerenciamento/alerta/automaçãoutilizado nos servidores e estações de trabalho;
- Sistema operacional dos servidores com acesso restrito ao administrador e sem navegação;
- Usuários sem acesso administrativo no equipamento, evitando assim instalação de softwareindesejado;
- Dados salvos diretamente na nuvem, onde é aplicada a rotina de retenção e versionamento;
- Sistema de rede wireless acessado através de software específico para gerenciamento/monitoramento;
- Para serviço de e-mail, a LIS Capital utiliza-se dos serviços contratados da Google Inc, o G Suite,configurado para usar o HTTPS, um protocolo seguro que fornece comunicação autenticadas e criptografadas com versões personalizadas de forma independente com o nome e domínio da LIS Capital.
- Rede sem fio com criptografia;
- Semanalmente, todos os arquivos localizados no serviço de armazenamento e partilha de arquivos baseado no conceito de “computação em nuvem” são copiados e arquivados, para uma pasta específica de backup na rede virtual Dropbox Business fornecido pela Dropbox Inc. contratada pela LIS Capital.
- Para o caso de documentos físicos, estes são digitalizados mensalmente e armazenados em pastas cujo acesso é restrito à pessoa responsável pela área administrativa da empresa. Outros colaboradores só terão acesso a esses documentos sob permissão e supervisão da pessoa responsável.
- Duplo fator de autenticação para acesso ao email corporativo.

6.4 MONITORAMENTO E TESTES

Os sistemas, serviços, dados, informações (incluindo as Informações Sigilosas) disponíveis na LIS Capitalpara serem usados pelos Colaboradores não devem ser interpretados como sendo de uso pessoal. Todos osColaboradores devem ter ciência de que o uso está sujeito à monitoramento periódico, inclusive em equipamentos pessoais acessados durante o expediente da Gestora, fazendo uso da sua rede ou não, sem frequência determinada ou aviso prévio. Esse monitoramento poderá ser realizado automaticamente(software e/ou hardware), pela Diretor de Risco, Compliance e PLDFT ou por prestador de serviços externo.

Abaixo estão listados os tipos de monitoramento e teste realizados pela LIS Capital:

- Monitoramento do ambiente tecnológico permanente;
- Trimestralmente é verificado se há novo firmware para o firewall, com avaliação das correções e oimpacto na sua atualização;
- Verificação dos logs dos Colaboradores;
- Segregação de acessos;
- No caso de falha em um link de internet, o link de redundância é ativado automaticamente.
- Manutenção trimestral de todo os hardwares; e
- Backup diário, realizado na nuvem.
- Atualizações do sistema operacional;
- Atualização/alerta do antivírus;
- Atualização de software de terceiros.

6.5 PLANO DE RESPOSTA

Havendo indícios ou de suspeita fundamentada, a empresa Tecnoqualify deverá ser acionada para realizar os procedimentos necessários de modo a identificar o evento ocorrido. Os procedimentos a serem aplicadospoderão variar de acordo com a natureza e o tipo do evento.

Na hipótese de vazamento de Informações Sigilosas ou outra falha de segurança, inclusive em decorrênciada ação de criminosos cibernéticos, as providências pertinentes deverão ser iniciadas de modo a sanar ou mitigar os efeitos no menor prazo possível.

Em caso de necessidade, poderá ser contratada empresa especializada para combater ao evento identificado.

Caso o evento tenha sido causado por algum Colaborador, deverá ser avaliada a sua culpabilidade, nos termos do Manual de Compliance e Código de Ética e Conduta.

7. PLANO DE CONTINUIDADE

Para minimizar perdas e evitar danos às atividades essenciais da empresa, a LIS Capital mapeou as contingências mais relevantes do negócio, e desenvolveu um Plano de Continuidade de Negócio visando permitir que a empresa, após a ocorrência de uma eventualidade ou desastre, reassuma o processamento das operações críticas dentro de um intervalo de tempo adequado às necessidades de negócio

I) Back-up e Recuperação de Dados: A LIS Capital mantém cópias eletrônicas de todas as informações fundamentais relacionadas aos fundos de investimento e seus investidores no seu servidor e em um ambiente seguro na "nuvem". Toda a informação eletrônica é arquivada diariamente e salva "online" no ambiente de contigência na nuvem. O diretor de Risco e Compliance é responsável pelo desenvolvimento de um arquivamento detalhado de dados e pelo plano de recuperação de desastres referente a todos os serviços de informações da LIS Capital e supervisiona a análise periódica deste plano;

II) Sistemas Críticos: Todos os sistemas que são cruciais para as operações de negócios da LIS Capital, incluindo, mas não limitados a sistemas que garantam processamento imediato das transações de valores mobiliários, manutenção de contas de clientes e acesso a contas de clientes, são considerados sistemas críticos de missão;

III) Nomeação do Centro de Comando Operacional: Na ocasião de uma emergência ou interrupção significativa nos negócios, a LIS Capital irá um endenreço alternativo que pode ser um novo escritório ou uma das residências de seus Colaboradores com acesso aos sistemas críticos de missão, ou outro local como seu centro de comando de operações, do qual os sistemas fundamentais serão tornados online e assim continuar os negócios da LIS Capital;

IV) Providências complementares e informações a clientes: Na ocasião de uma emergência ou outra interrupção de negócios significativa, a LIS Capital irá contatar o Administrador e Investidores a fim de informar da condição da LIS Capital e de oferecer informações de contato através dos quais a LIS Capital pode ser contatada, o quanto antes possível;

V) Relatórios Regulamentares e Comunicação com Reguladores: Na ocasião de uma emergência ou interrupção de negócios significativa, a LIS Capital irá contatar todos os órgãos Reguladores que supervisionam a LIS Capital, para informar tais órgãos da situação da LIS Capital, e para fornecer informações de contato através dos quais a LIS Capital pode ser contatada. O diretor de Risco e Compliance é nomeado como pessoa de contato da LIS Capital para lidar com comunicações com reguladores. Caso o diretor de Risco e Compliance não possa se comunicar com os reguladores, outro colaborador irá assumir tal responsabilidade.

VI) Contingências com servidor de e-mail: O servidor da LIS Capital é baseado na "nuvem", o que implica acesso de qualquer ponto com internet, independente da localização. O serviço utilizado tem backups online protegido por sistema de encripção.

8. VIGÊNCIA E ATUALIZAÇÃO

Esta Política de Segurança Cibernética e Contingêncua será revisada anualmente, e sua alteração acontecerá caso seja constatada necessidade de atualização do seu conteúdo. Poderá, ainda, ser alterada a qualquer tempo em razão de circunstâncias que demandem tal providência. Qualquer alteração à presente Política seráamplamente divulgada a todos os Integrantes da LIS Capital pelo Diretor de Risco, Compliance & PLDFT que é o responsável pelas questões de segurança cibernética.