



EXPLORITAS

EXPLORITAS ADMINISTRAÇÃO FINANCEIRA LTDA

MANUAL DE CIBERSEGURANÇA

Dezembro 2019

O NÃO CUMPRIMENTO DESTE MANUAL PODERÁ RESULTAR EM AÇÕES DISCIPLINARES APROPRIADAS, INCLUINDO ADVERTÊNCIAS, QUE PODERÃO VIR A CULMINAR NO DESLIGAMENTO DA EMPRESA. ESTE MANUAL NÃO É DESTINADO A CRIAR QUALQUER CONTRATO DE TRABALHO ENTRE A EMPRESA E QUAISQUER DE SEUS MEMBROS.

Revisões

Revisão	Data	Alteração	Responsáveis
00	12/2018	Criação do Documento	Murad Antun
01	12/2019	Revisão do Documento	Murad Antun

Objetivos

Esta política (“Política”) tem por objetivo estabelecer critérios de identificação de riscos cibernéticos e orientar atividades que mitigam o risco e que possam recuar o funcionamento normal da empresa em caso possíveis incidentes.

De forma mais abrangente, a Exploritas Administração Financeira Ltda (“Exploritas”) entende que o tratamento de cibersegurança anda em conformidade com os procedimentos adotados em nosso manual de segurança da informação (disponível no site da Exploritas: www.exploritas.com.br).

A Política define, ainda as competências, responsabilidades e atribuições dos envolvidos nos processos de mitigação e endereçamento do risco cibernético.

Avaliação de Riscos

Abaixo abordamos os riscos internos e externos à gestora relacionados ao hardware, ao software e a processos que necessitam de proteção.

Em termos de hardware, a Exploritas possui rede interna de dados que pode sofrer ataques de diferentes formas. A telefonia IP da empresa está vinculada à rede interna de dados.

Em termos de software, os aplicativos fundamentais são utilizados para a condução dos investimentos dos fundos geridos. rotinas de trading, alocações e boletagens, as quais podem ser afetadas.

Embora não haja a condução da atividade de distribuição, retemos informações de clientes de Distribuição Direta, as quais poderiam ser alvo de extravio de informações confidenciais.

Ações de Proteção e Prevenção

O acesso aos computadores de nossa rede se dá mediante senha de 8 dígitos ou mais, contendo letras e números, com política de renovação periódica, a qual veda utilização de seis senhas anteriores.

Todos os dispositivos da gestora estão conectados a uma rede de Internet de banda larga que está sempre ativa. Utilizamos um firewall de borda SonicWall parametrizado pelas áreas de Compliance e TI para utilização de bandas para Bloomberg, telefonia e dados.

O servidor de rede é protegido fisicamente por rack chaveado, cujo acesso somente ocorre através da área de Compliance.

Todas as máquinas utilizam o antivírus Kaspersky atualizado constantemente em toda a rede.

Nossa telefonia se utiliza do serviço de PABX em nuvem da Locaweb. As ligações dos telefones de execução de trades e comercial são gravadas com as devidas retenções históricas. Além disto, temos os softphones nos celulares para redundância. Outra linha analógica também está disponível para redundância.

Em relação aos softwares, buscamos garantir que sempre estaremos utilizando as últimas versões disponíveis. Nosso parque tecnológico é gerenciado por um administrador de sistemas, que verifica regularmente a atualização de todos os clientes da rede e do servidor. Atualizações automáticas ocorrem regularmente (semanal ou a cada disponibilização ou a cada vez que as máquinas são reiniciadas).

Na condução das atividades fudaentaos à Gestão dos ativos do fundo, utilizamos terminais Bloomberg e o EMSX como blotter. Há blotter redundante com escripts VBA caso tenhamos dificuldades de acesso. A captura destas operações e conciliações se dá via módulo da Lote 45. Tanto Bloomberg quanto o Lote 45 são provedores de software que podem ser acessados remotamente via Bloomberg Anywere e liberação de IPs pelo Diretor de Compliance junto à Lote45. Como redundância neste proceso temos dropcopy via SFTP com três corretoras mapeadas. Esta comunciação é criptografada e conduzida em ambiente seguro.

Em relação às informações de nossos clientes, os e-mails trocados são armazenados junto ao provedor da Google e passam pela análise de antivírus antes de sua abertura. Os dados de cadastro são protegidos pela estrutura de direitos de acesso em nossa rede.

Ainda, segundo nosso manual de Segurança da Informação, mantemos 5 backups diários em diferentes locais (servidor, gavetas de 4T e nuvem).

Monitoramento e Testes

A empresa tem por política realizar inspeções independentes, conduzidas por um terceiro contratado de no mínimo uma vez a cada biênio, com objetivo de testar a adequação dos recursos de tecnologia da informação, para assegurar o cumprimento das Diretrizes e Procedimentos dessa Política e atualizar e recomendar quaisquer alterações nos controles, políticas e procedimentos adotados.

Os registros de tais assessments ficarão armazenados na sede da gestora por prazos superiores a dois anos.

Plano de Resposta

Em caso de um possível incidente, o responsável pela identificação do incidente em questão deverá comunicar o Diretor de Compliance imediatamente para que este possa avaliar impactos e acionar as medidas necessárias.

É de responsabilidade do Diretor de Compliance receber, analisar e responder às notificações e atividades relacionadas aos incidentes de segurança na rede de computadores da Exploritas, assim como coletar e anexar todas as evidências necessárias para a solução ou prevenção dos incidentes.

O processo de resposta a incidentes desempenhado deverá ser constantemente documentado de forma a aferir os serviços realizados e absorver lições aprendidas de cada situação.

Revisões

O Diretor de Compliance revisará a Política de Cibersegurança no mínimo anualmente e, sempre que alterações forem realizadas, aprovadas e colocadas em vigor, as mesmas deverão ser amplamente divulgadas para todos os colaboradores.