SPECTRA INVESTMENTS

Política de Segurança Cibernética

Março 2024

Esta Política de Segurança Cibernética tem como objetivo delinear as regras e os procedimentos que visam garantir a integridade, disponibilidade e confidencialidade dos dados utilizados pelos colaboradores da Spectra Investimentos Ltda. ("SPECTRA").

I. Avaliação de Riscos

a. Identificação de ativos relevantes

Telefonia: a linha telefônica utilizada é fornecida por terceiros e permite acesso remoto a qualquer ponto conectado à internet. Esse acesso é possível através da utilização de senhas, que ficam em posse dos diretores. O sistema é protegido pela separação dos sinais de sinalização e voz em endereços IP distintos. Além disso, é feito o monitoramento de quais IPs são normalmente utilizados, a fim de garantir que a linha não esteja sendo desviada nem monitorada.

E-mail: utilizamos sistema de e-mails com as certificações internacionais mais rigorosas de segurança, privacidade e *compliance*. Os acessos são feitos em qualquer dispositivo com conexão à internet, através de um sistema criptografado e protegido de ataques externos.

Servidores: os dados da empresa provêm tanto do servidor físico quanto do servidor em nuvem. Os servidores funcionam em paralelo, a fim de garantir a redundância do registro das informações em tempo real.

Informações pontuais: dados que dizem respeito a aspectos específicos das partes relacionadas. São informações normalmente recebidas via e- mail, que não apresentam grande sensibilidade devido ao baixo potencial de utilização isolada.

Informações coletivas: arquivos/informações que contêm dados agregados internos e externos. São armazenadas nos servidores em nuvem, descritos acima, apenas pelos computadores da empresa.

b. Potenciais riscos

Perda de confidencialidade: vazamento de informações em geral, podendo comprometer partes internas e externas à organização. Essa perda

pode ocorrer tanto com informações pontuais quanto com informações agregadas.

Perda de integridade: alterações de informações de maneira a comprometer as análises e conclusões da empresa.

Perda de disponibilidade: impedimento do acesso às informações devido a restrições físicas ou tecnológicas, prejudicando o funcionamento da empresa.

c. Cenários de ameaças

Ameaças externas: são ameaças provenientes de terceiros, visando o monitoramento ou adulteração das informações utilizadas.

Ameaças internas: ameaças provenientes do uso interno das informações, podendo ser intencionais ou não-intencionais.

II. Ações de proteção e prevenção

Políticas internas: a "*Política de segurança e confidencialidade"* e o "*Código de ética"*, assinados por todos os colaboradores, estipulam, entre outros termos, que o responsável arcará com os custos associados ao vazamento das informações quando comprovado o vazamento intencional de informações.

Controle de portas USB: a utilização das portas só é permitida acima de determinados tamanhos de transferência, com a autorização dos diretores, através do uso de senha para desbloqueio.

Controle de instalação de softwares: só é permitida a instalação de softwares autorizados pela área de TI, através da concessão de privilégios de administrador nos computadores utilizados. Periodicamente são realizadas varreduras para conferência da aderência às restrições.

Acesso às informações: informações coletivas só podem ser acessadas através dos usuários e senhas da empresa junto ao Microsoft 365. Nos computadores há diferentes níveis de informação permitida para cada usuário, compatíveis com as áreas de atuação. Essas permissões são definidas e concedidas pelos diretores.

Acesso remoto: o acesso é realizado por meio de rede criptografada, através de usuários, garantindo a rastreabilidade das ações realizadas na rede.

Firewall: utilizado para a prevenção de ataques externos aos servidores internos, mesmo que a comunicação com os servidores seja criptografada.

Segregação de Informações: Diferentes níveis de acesso a pastas internas são dados para os colaboradores da organização. Para profissionais que não sejam sócios da empresa, seu acesso é restrito apenas às pastas com cujas informações trabalhe no dia-a-dia.

Ainda, toda movimentação de arquivos é monitorada, caso haja alguma movimentação suspeita, isto é, em massa e de locais não normais, o Diretor de Compliance é notificado imediatamente. Todos os sistemas permitem corte de acesso instantâneo, bem como possuem criptografia ponta a ponta para evitar vazamentos em transferências.

III. Mecanismos de supervisão

Testes de Backup: são realizados periodicamente a fim de garantir o bom funcionamento dos sistemas.

Monitoramento: periodicamente são analisados os registros de acessos, analisando se o padrão apresenta alguma tentativa de prática maliciosa. Também são monitorados os softwares instalados, de modo a verificar sua conformidade com as políticas estabelecidas pela SPECTRA.

Testes de Phishing: periodicamente executados pela área de TI com todos os colaboradores e sem comunicação prévia.

IV. Plano de resposta a incidentes

Ameaça externa: a área de TI será acionada para que sejam identificadas as vulnerabilidades e informações alteradas/consultadas. Caso necessário será realizado o bloqueio do acesso às informações, permitido somente através de novos usuários. Poderá também ser restaurado o Backup a fim de garantir a integridade das informações.

Ameaça interna: serão acionados os diretores e área de TI de modo a rastrear e apurar os possíveis danos causados às informações. O responsável estará sujeito às medidas estabelecidas na *"Política de Confidencialidade"* e *"Código de Ética",* de acordo com as apurações prévias.

V. Responsável por tratar e responder questões de segurança cibernética.

Responsável: Rafael Honório Bassani, sócio-diretor responsável pela área de Risco e Compliance.

Data	Alterações	Versão
28/03/2024	Revisão da política	5