DIRETRIZES DA POLÍTICA DE SEGURANÇA CIBERNÉTICA

ADG

DATA 11/11/2024

1 Objetivo

O conhecimento, em nossa visão, é chave à manutenção de um ambiente cibernético seguro e confiável. Nesse contexto, buscamos, por meio desta carta, compartilhar as linhas gerais das medidas e procedimentos de segurança cibernética adotados pela Corretora ("Diretrizes"), com os quais recomendamos que nossos clientes e usuários busquem se familiarizar.

A informação apresentada neste Arquivo de Governança ("**ADG**") visa proteger e fomentar o ambiente computacional em nuvem seguro, buscando conscientizar quanto aos controles e procedimentos implementados pela Corretora com o intuito de reduzir as vulnerabilidades de eventuais incidentes relacionados ao ambiente cibernético buscando compatibilização com melhores práticas de mercado e regulamentações aplicáveis.

Recomendamos, em complemento, a leitura dos demais documentos de segurança da informação e cibernética disponíveis em nosso website, como o documento Boas Práticas de Navegação na Internet, que estabelece linhas gerais de segurança da informação para a navegação segura de nossos clientes e usuários.

2 Principais Ações, Controles e Processos adotados pela Corretora (Segurança Cibernética)

Para assegurar que as informações tratadas estejam protegidas a Corretora adota as seguintes ações, controles e processos:

I. Assegura os 3 (três) pilares de segurança da informação: confidencialidade, integridade e disponibilidade das informações dos clientes, prestadores de serviço e colaboradores adotando mecanismos de segurança adequados;

II. Possui procedimentos e controles no plano de resposta à incidentes em caso de interrupção de serviço relevante considerando os cenários dos testes de continuidade de negócio realizados;

III. Adota procedimentos de gerenciamento de riscos para mitigar os efeitos dos incidentes relevantes de processamento, armazenamento de dados e de computação em nuvem;

IV. Possui mecanismo de acompanhamento, monitoração e de controle dos processos para assegurar a implementação e a efetividade da política de segurança cibernética, plano de ação e de respostas a incidentes e requisitos para contratação de serviços de processamento e armazenamento de dados e de computação em nuvem;

V. Tem iniciativas para o compartilhamento de informações sobre os incidentes relevantes;

VI. Dissemina a cultura entre os colaboradores, prepostos e prestadores de serviços para atender ao programa de conscientização de Segurança Cibernética;

VII. Adota estratégias e tecnologias alinhadas com os processos de classificação das informações, que tem como objetivo criar controles para coibir o vazamento da informação durante o processamento e o tráfego dos dados com objetivo de prevenir a exfiltração de informação;

VIII. Tem mecanismos de segurança para proteção de ataques cibernéticos e prevenção a instalação não autorizada softwares maliciosos a fim de assegurar contra vulnerabilidades do ambiente tecnológico;

IX. Tem procedimentos e controles de descarte e manutenção segura de dados, equipamentos e mecanismos de segurança que assegurem a proteção contra acesso indevido, cópia ou modificação não autorizada;

X. Define procedimentos e controles voltados a prevenção e ao tratamento dos incidentes adotados por empresas prestadoras de serviços a terceiros que manuseiam dados ou informações sensíveis ou que sejam relevantes para condução das atividades operacionais;

XI. Define controles para prevenir, detectar, reduzir e tratar incidentes de Segurança Cibernética;

XII. Define a criticidade do serviço e a sensibilidade dos dados e das informações a serem processadas, armazenadas e gerenciadas pelo contratado, levando em conta, inclusive, a classificação realizada de acordo com sua relevância baseado o impacto dos efeitos do incidente;

XIII. Comunica, sempre que aplicável, de forma tempestiva os reguladores autorreguladores e ambientes de mercado das ocorrências de incidentes de Segurança Cibernética relevantes e das interrupções dos serviços relevantes, que configurem uma situação de crise, bem como das providências para o reinício das atividades de acordo com a norma de Gestão de Incidentes e Problemas interna;

XIV. Adota práticas de governança corporativa e de gestão proporcionais à relevância do serviço a ser contratado e aos riscos a que estejam expostos; e

XV. Avalia se as partes contratadas pela Corretora possuem, onde aplicável, processos e procedimentos que garantam a disponibilidade, integridade e confidencialidade das informações processadas e/ou armazenadas e que estes preservem documentação suficiente para demonstrar que seus processos e controles estão adequados e aptos para prestar de forma segura os serviços contratados.

3 Diretrizes da Política de Segurança Cibernética da Corretora

As Diretrizes da Política de Segurança Cibernética da Corretora podem ser apresentadas conforme a seguir:

I. **Identificação e Autenticação -** mecanismos que garantem a autenticidade e rastreabilidade dos usuários na utilização dos recursos computacionais. Ou seja, tornam possível a identificação dos autores de qualquer ação feita utilizando os sistemas informatizados e meios de comunicação;

II. **Criptografia -** mecanismo de segurança e privacidade que torna determinada comunicação (e.g., textos, imagens, vídeos) inacessível para quem não tem acesso aos códigos de codificação, o qual chamamos de chave criptográfica ou “tradução” da mensagem;

III. **Prevenção e Detecção de Intrusão -** tecnologias projetadas para monitorar toda atividade de entrada e saída de uma rede de dados, identificando quaisquer padrões suspeitos de tráfego que podem indicar uma tentativa de ataque;

IV. **Prevenção de Vazamento de Informações -** processos para o controle da informação na sua utilização, compartilhamento e tráfego e detecção de possíveis violação de dados;

V. **Varreduras para Detecção de Vulnerabilidades -** procedimentos de detecção de eventuais pontos de fragilidade, que, caso explorados, podem comprometer a confidencialidade, a disponibilidade e a integridade das informações de um indivíduo ou empresa;

VI. **Proteção contra Softwares Maliciosos -** tecnologias e soluções que visam a garantir proteção a dispositivos (celular, tablet, notebooks etc.) não estejam vulneráveis a ataques de hackers ou danificados por programas maliciosos;

VII. **Mecanismos de Rastreabilidade -** monitoramento do tráfego de informações e recursos de processamento, a fim de verificar sua normalidade, assim como detectar situações anômalas do ponto de vista da segurança cibernética;

VIII. **Segmentação da Rede -** segregação de rede é dividida em vários segmentos de segundo nível de acesso e isolados com objetivo de mitigar riscos de disseminação de tráfego de rede em caso de comprometimento de parte da estrutura;

IX. **Manutenção das Cópias de Segurança -** processo de cópia de dados de um dispositivo de armazenamento a outro, para que possam ser restaurados em caso de perda dos dados originais;

X. **Registro e Análise de Impacto de Incidentes Ocorridos -** processo que visa a gerenciar a ocorrência de incidentes na infraestrutura de tecnologia da informação, com a finalidade de prover monitoramento, correção e melhoria de processos. Consiste, de modo geral, em registrar e analisar a causa dos incidentes ocorridos, fornecendo soluções em tempo hábil e evitar sua recorrência, minimizando e/ou evitando seu impacto;

XI. **Controles de Acesso -** tecnologia e procedimentos que visam a permitir ou negar a utilização de um ambiente (equipamento ou sistema) por uma pessoa (usuário ou um processo) limitando os acessos não autorizado com objetivo de proteger este ambiente;

XII. **Disseminação da Cultura de Segurança Cibernética -** engajamento interno ativo da Corretora visando a capacitação contínua e conscientização de seus colaboradores, parceiros, clientes e usuários. Inclui a disseminação contínua de informações, atividades de treinamento, medir o conhecimento dos colaboradores e, de maneira abrangente, uma variedade de mecanismos de governança e processos a garantir aderência e conformidade.

Forma de Divulgação: Este ADG estará disponível para consulta do público no website da Corretora.

Importante: Para outras dúvidas entre em contato com a Corretora através da caixa de contatos disponível na página web da Corretora.

Versão	Data	Descrição
01	04/12/2020	Versão inicial
02	12/12/2022	Versão anterior aprovada sem ajustes relevantes
03	16/05/2023	Inclusão de seção Ações, processos e controles e reformatação do arquivo.
04	11/11/2024	Revisão anual do documento, sem alterações.