POLÍTICA CORPORATIVA DE SEGURANÇA DA INFORMAÇÃO E SEGURANÇA CIBERNÉTICA

Objetivo

A Política de Segurança da Informação e Segurança Cibernética, é o documento que orienta e estabelece as diretrizes corporativas da Broker Brasil para a proteção dos ativos de Informação e a prevenção de responsabilidade legal para todos os usuários. Deve, portanto, ser cumprida e aplicada em todas as áreas da instituição.

A estratégia de Segurança da Informação e Segurança Cibernética foi desenvolvida para evitar violações da segurança dos dados, minimizar os riscos de indisponibilidade dos nossos serviços, proteger a integridade e evitar qualquer vazamento de informação. Para alcançarmos esse objetivo implantamos os processos de controle para detecção, prevenção, monitoramento e resposta a incidentes garantindo a gestão do risco de segurança cibernética. Estes processos de controle consideram que a informação deve ser protegida independentemente de onde ela esteja, seja em um prestador de serviço ou na própria Corretora.

A presente está baseada nas recomendações propostas pela norma ABNT NBR ISO/IEC 27002:2013, reconhecida mundialmente como um código de prática para a gestão da segurança da informação, bem como está de acordo com as leis vigentes em nosso país e com a Resolução n° 4.658 de 26 de abril de 2018.

Estabelecer diretrizes que permitam aos funcionários, colaboradores e clientes da Broker Brasil seguirem padrões de comportamento relacionados à segurança da informação adequados às necessidades de negócio e de proteção legal da empresa e do indivíduo.

Nortear a definição de normas e procedimentos específicos de segurança da informação, bem como a implementação de controles e processos para seu atendimento.

Preservar as informações quanto aos princípios da segurança da informação da Broker Brasil quanto à:

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.*

b. ***Confidencialidade****: garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.*

c. ***Disponibilidade:*** *garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.*

Público

Todos os funcionários, colaboradores e prestadores de serviços da Broker Brasil Corretora

Regra Geral

A política de segurança da informação e segurança cibernética precisa estar disponível em local acessível aos funcionários e colaboradores.

A política de segurança da informação e segurança cibernética é revisada anualmente pela Broker Brasil.

Diretrizes de Segurança da Informação Segurança Cibernética

A Segurança da Informação e Segurança Cibernética na Broker Brasil estabelece as seguintes diretrizes:

a. As informações da Corretora, dos clientes e do público em geral devem ser tratadas de forma ética e sigilosa e de acordo com as leis vigentes e normas internas, evitando-se mau uso e exposição indevida.

b. A informação deve ser utilizada de forma transparente e apenas para a finalidade para a qual foi coletada.

c. Todo processo, durante seu ciclo de vida, deve garantir a segregação de funções, por meio da participação de mais de um colaborador ou equipe de colaboradores, para que a atividade não seja executada e controlada pelo mesmo colaborador ou equipe.

d. O acesso às informações e recursos só deve ser feito se devidamente autorizado.

I. A identificação de qualquer funcionário e Colaborador deve ser única, pessoal e intransferível, qualificando-o como responsável pelas ações realizadas.
II. A concessão de acessos deve obedecer ao critério de menor privilégio, no qual os usuários têm acesso somente aos recursos de informação imprescindíveis para o pleno desempenho de suas atividades.
III. A senha é utilizada como assinatura eletrônica e deve ser mantida secreta, sendo proibido seu compartilhamento.
IV. Todo colaborador deve reportar os riscos às informações à área de Segurança da Informação e segurança cibernética.

V. A área de Segurança de Informação e segurança cibernética deve divulgar amplamente as responsabilidades sobre Segurança da Informação e cibernética aos funcionários e Colaboradores, que devem entender e assegurar estas diretrizes.

Processo de Segurança da Informação e Segurança Cibernética

Para assegurar que as informações tratadas estejam adequadamente protegidas, a Broker Brasil adota os seguintes processos:

a. Gestão de Ativos da Informação

- Entende-se por Ativos da Informação tudo o que pode criar, processar, armazenar, transmitir e até excluir a informação. Podem ser tecnológicos ("software" e "hardware") e não tecnológicos (pessoas, processos e dependências físicas).
- Os ativos da informação, de acordo com sua criticidade, devem ser identificados de forma individual, inventariados e protegidos de acessos indevidos, fisicamente (salas com acesso controlado) e logicamente (configurações de blindagem ou "hardening", patch management, autenticação e autorização).

b. Gestão de Acessos

- As concessões, revisões e exclusões de acesso devem utilizar as ferramentas e os processos da Corretora.
- Os acessos devem ser rastreáveis, a fim de garantir que todas as ações passíveis de auditoria possam identificar individualmente o Colaborador, prestador de serviço, para que seja responsabilizado por suas ações.

c. Gestão de Riscos

- Os riscos devem ser identificados por meio de um processo estabelecido para análise de vulnerabilidades, ameaças e impactos sobre os ativos de informação da Corretora.
- Os cenários de riscos de segurança da informação são acompanhados e definidos pelo responsável das áreas envolvidas e pelo Comitê de Riscos.

d. Tratamento de Incidentes de Segurança da Informação e Segurança Cibernética

- A área de Segurança da Informação e Segurança Cibernética realiza a monitoração de segurança do ambiente tecnológico da Broker Brasil, analisando os eventos e alertas com o objetivo de identificar possíveis incidentes.

- Os incidentes que são identificados pelos alertas são classificados com relação ao impacto de acordo com os critérios adotados pela Corretora. Para o seu grau de relevância serão considerados aspectos como comprometimento de dados de clientes e impacto ao sistema financeiro.
- Todos os incidentes passam por um processo de tratamento e comunicação, onde são registradas todas as informações pertinentes aos incidentes como causa, impacto, classificação, etc, de acordo com o procedimento operacional.
- Visando aprimorar a capacidade da Corretora na resposta a incidentes cibernéticos, alguns cenários que possam afetar a continuidade de negócios são considerados nos testes.
- A área de Riscos elaborará um Relatório Anual contendo os incidentes relevantes ocorridos no período, ações realizadas de prevenção e respostas aos incidentes e resultados dos testes de continuidade. Este relatório deverá ser apresentado ao Comitê de Riscos.

e. Conscientização em Segurança da Informação e Segurança Cibernética

A Corretora promove através de e-mail periodicamente a disseminação dos princípios e diretrizes de Segurança da Informação por meio de programas de conscientização, com o objetivo de fortalecer a cultura de Segurança da Informação.

f. Governança com as Áreas de Negócio e Tecnologia

As iniciativas e projetos das áreas de negócio e tecnologia devem estar alinhadas com as diretrizes e arquiteturas de segurança da informação, garantindo a confidencialidade, integridade e disponibilidade das informações.

g. Segurança Física do Ambiente

O processo de Segurança Física visa estabelecer controles relacionados à concessão de acesso físico ao ambiente somente a pessoas autorizadas, de acordo com a criticidade das informações previamente mapeadas e declaradas à sede Administrativa.

h. Gravação de LOGs

É obrigatória a gravação de logs ou trilhas de auditoria do ambiente computacional de forma a permitir identificar: quem fez o acesso; quando o acesso foi feito; o que foi acessado e como foi acessado.

As informações dos registros (logs) ou trilhas de auditoria devem ser protegidas contra modificações e acessos não autorizados.

i. Proteção de perímetro

Para proteção da infraestrutura da Corretora contra um ataque externo, utilizamos ferramentas e controles contra: ataques que afetem a disponibilidade, Spam, Phishing, ataques avançados persistentes (APT), Malware, invasão de dispositivos de rede e servidores, ataques de aplicação e scan externos.

Avaliação Independente da Auditoria

A efetividade das políticas de Segurança da Informação é verificada por meio de avaliações periódicas de Auditoria Interna.

Declaração de Responsabilidade

Periodicamente os Colaboradores e Prestadores de Serviços diretamente contratados pela Corretora devem aderir formalmente a um termo, comprometendo-se a agir de acordo com as políticas de Segurança da Informação.

Os contratos firmados com a Broker Brasil devem possuir cláusula que assegure a confidencialidade das informações.

Medidas Disciplinares

As violações a esta política estão sujeitas às sanções disciplinares previstas nas normas internas da Broker Brasil, e na legislação vigente no Brasil.