Política de Segurança da Informação da EQI CTVM

Sumário

1. Objetivo da Política

A presente Política de Segurança da Informação ("Política") da EQI Investimentos Corretora de Títulos e Valores Mobiliários S.A. ("EQI CTVM") tem como objetivo estabelecer a base para o programa de segurança da informação, cuja essência é aplicar medidas economicamente eficientes que protejam os ativos da EQI CTVM com um nível aceitável de risco residual.

Esta Política se aplica aos colaboradores, prepostos e terceiros da EQI CTVM, incluindo aqueles de empresas subsidiárias sob a gestão EQI CTVM.

2. Princípios

Entende-se como segurança da informação o conjunto de medidas que visam garantir a identificação, resposta e recuperação do incidente de segurança da informação, garantindo assim a continuidade dos negócios. Tais medidas devem impedir o uso, divulgação, alteração ou destruição não autorizada de informações.

Os controles estabelecidos, visam evitar ações que comprometam a imagem da EQI CTVM e/ou perdas financeiras decorrentes de falhas tecnológicas considerando os seguintes pilares:

(i) **Confidencialidade**: Garantir que todos os meios de processamento e ou conservação de informação contenham medidas de proteção quanto ao acesso e utilização por pessoa não-autorizada, assegurando com isso que toda informação esteja protegida de revelações acidentais, espionagem industrial, violação da privacidade e outras ações similares;

(ii) **Integridade**: Assegurar que toda informação processada em cada um dos sistemas de informação e processos transacionais seja necessária, útil e suficiente para o desenvolvimento dos negócios. Esteja livre de erros ou irregularidades, de qualquer espécie;

(iii) **Disponibilidade**: Garantir que a informação e sua capacidade de processamento, manual e automática, sejam resguardadas e recuperadas sempre que necessário, de modo a não impactar significativamente o andamento dos negócios;

(iv) **Conformidade**: Assegurar que toda informação e os meios físicos que a contenham, processem e ou transportem, cumpram com

os regulamentos legais vigentes em cada âmbito, e que todos os direitos de propriedade sobre a informação utilizada ou produzida pela EQI CTVM, no desenvolvimento de suas atividades, estejam adequadamente estabelecidos a favor da empresa.

3. Classificação da Informação

A informação pode estar presente em sistemas e diversos tipos de mídias, tais como: documentos eletrônicos, e-mail, papel, mídias removíveis (CD, DVD, Pen Drive), microfilme e por meio da comunicação verbal.

As informações, bem como os ativos que a suportam, devem ser classificados segundo seu nível de importância para a organização e protegidas de forma adequada.

Para garantir a proteção adequada das informações, é fundamental classificá-las de acordo com sua importância estratégica para os negócios da EQI CTVM, aplicando o nível de confidencialidade apropriado conforme essa classificação:

(i) **Informação pública (Public)**: refere-se a dados e conteúdos destinados ao público em geral que já foram oficialmente divulgados pela empresa. Caracteriza-se por ser de livre acesso, não necessitando de autorização prévia do titular para sua utilização, e por não apresentar potencial de causar danos ou prejuízos à organização quando divulgada ou compartilhada. Exemplos: Apresentações institucionais que não contenham dados financeiros sensíveis, informações sobre eventos, comunicados à imprensa, materiais promocionais e de marketing.

(ii) **Informação interna (Confidential - internal use only)**: refere-se a informações de uso exclusivo da empresa, com acesso restrito aos colaboradores internos. Embora a empresa não tenha interesse em divulgar esse conteúdo externamente, sua eventual exposição não representa risco significativo de prejuízos organizacionais. Exemplos: Diretrizes institucionais, plano estratégico, política de viagens, política de compras.

(iii) **Informação restrita (Highly confidential – recipients only):** refere-se a informações de caráter sigiloso e estratégico, cujo acesso é limitado exclusivamente aos colaboradores que possuam necessidade

profissional para o desempenho de suas funções na empresa, sua eventual exposição pode causar perda de clientes e oportunidades, prejuízos financeiros e comprometimento da reputação e imagem corporativa. Exemplos: Relatórios executivos, documentos societários, planos estratégicos, informações de clientes.

(iv) **Informação confidencial (Highly confidential - data privacy)**: refere-se a informações de natureza sigilosa e estratégica, cujo acesso é restrito exclusivamente às pessoas formalmente autorizadas e designadas para tal função. Caracteriza-se por conter dados de importância crítica para a organização e seus stakeholders, cuja divulgação não autorizada pode resultar em prejuízos significativos de ordem moral, patrimonial, operacional ou reputacional para a empresa. Exemplos: Dados financeiros e contábeis estratégicos, dados pessoais de colaboradores e clientes (LGPD), salários, código-fonte, banco de dados e procedimentos e protocolos de segurança.

4. Responsabilidades e procedimentos

Todos os colaboradores, propostos e terceiros são responsáveis pela segurança da informação em sua área de trabalho e na instituição.

Todas as informações geradas e manuseadas pelos colaboradores, prepostos e terceiros da EQI CTVM no exercício de sua função são de propriedade da EQI CTVM. Portanto, devem manuseá-las de forma correta respeitando a sua classificação, protegendo-a com atenção. Para tanto é de responsabilidade dos colaboradores e parceiros da EQI CTVM:

(i) Tomar conhecimento da presente Política;

(ii) Cumprir as determinações da presente Política;

(iii) Respeitar o caráter confidencial das senhas de acesso aos ativos de tecnologia da informação ("TI") que lhe forem concedidas;

(iv) Utilizar os ativos de TI única e exclusivamente para os fins a que foram destinados;

(v) Utilizar das informações apenas dentro dos limites de sua autorização e para os propósitos para os quais as informações foram fornecidas;

(vi) Manter a confidencialidade, a integridade e a disponibilidade das

informações durante e após o seu envolvimento com a EQI CTVM;

(vii) Comunicar à equipe de segurança da informação, ao superior imediato, ao gerente da área, ou à área de TI as ocorrências que afetem, ou possam vir a afetar, a segurança ou o desempenho do ambiente de TI.

Quando o funcionário possuir entre as suas responsabilidades a gestão de pessoas que acessam informações, ou interagem de maneira habitual ou ocasional com os ativos de TI na execução de suas tarefas, devem também:

(i) Disponibilizar a presente Política para conhecimento de todo colaborador sob sua gestão;

(ii) Assegurar o cumprimento da presente Política por todo colaborador, sob sua gestão;

(iii) Requisitar o acesso às informações, somente no nível necessário, para a execução da atividade de seu colaborador;

(iv) Solicitar o imediato cancelamento do acesso de todo o colaborador, sob a sua gestão, que seja desligado ou transferido de função.

5. Acesso à Rede, Sistemas e Utilização de Recursos de TI

A EQI CTVM possui a "*PCA - Política de Controle de Acesso.pdf*" que trata do processo de concessão e controle dos usuários rede, sistemas, aplicações e recursos de TI.

O uso de senhas para acesso aos recursos tecnológicos é de responsabilidade do colaborador. A área segurança da EQI CTVM, realiza o monitoramento do ambiente por meio de registros de auditoria em computadores, sistemas, mensagens eletrônicas, acessos à internet, entre outros. Essas informações podem ser coletadas e utilizadas, a critério da EQI CTVM, para a execução de investigações internas ou para atendimento de medidas judiciais, sem aviso prévio às pessoas envolvidas, respeitando-se, porém, a privacidade dos colaboradores.

A utilização de mídias removíveis (pen drives, CD's, DVD's etc.) é restrita somente às pessoas que necessitem desse recurso para desenvolver suas atividades.

5.1. Renúncias / exceções

As exceções de acesso à sistemas e recursos de TI devem ser formalizadas mediante abertura de ticket e aprovada previamente, seguindo a cadeia de aprovação abaixo:

(i) Líder direto do Solicitante;

(ii) Diretor da Área;

(iii) Diretor Proprietário da Informação;

(iv) Responsável pela Área de Compliance;

(v) Diretor de TI.

6. Segregação Física

Por conta do modelo operacional adotado pela EQI CTVM em parceria com a PNP, não possuímos mesa de operações e/ou sessões de negociação. Consequentemente, a segregação do ambiente de processamento não é aplicável ao nosso contexto operacional.

Essa abordagem garante que todos os requisitos regulatórios sejam atendidos, mantendo a eficiência e segurança das operações. A EQI CTVM assegura que o PNP contratado cumpre todas as normas de segurança e regulatórias aplicáveis, garantindo assim a proteção e a integridade dos dados e processos sob sua responsabilidade.

7. Plano de Comunicação

Quando confirmado um incidente de segurança da informação no ambiente tecnológico da EQI CTVM, este deverá ser devidamente registrado no sistema de chamados, classificado de acordo com sua criticidade e impacto e determinado o formato da comunicação que será adotada de acordo com as partes envolvidas.

7.1 Comunicação

(i) Clientes

A comunicação com o cliente será realizada até duas horas após confirmado o incidente se segurança da informação.

(ii) Colaboradores

Durante eventual incidente a comunicação com os colaboradores é realizada através de e-mail, televisores institucionais, lives e/ou pessoalmente.

(iii) Reguladores

Em até oito horas após confirmado o incidente de segurança da informação a EQI CTVM reportará aos reguladores e Superintendência de Relação com o Mercado e Intermediários (SMI) a causa, impacto, medidas adotadas, e plano de ação para tratar o incidente de segurança da informação.

7.2 Canais de Comunicação

Os canais de comunicação serão estabelecidos de acordo com a disponibilidade em um eventual incidente de segurança da informação, conforme abaixo:

(i) Comunicação com contatos externos

A EQI CTVM determina que a comunicação com os contatos externos deve ser realizada de acordo com os canais e responsabilidades abaixo:

a. Imprensa: Nenhum colaborador está autorizado a falar com a imprensa. Todas as questões devem ser direcionadas para a área de relações públicas.

b. Agências regulatórias: Colaborares autorizados da área de compliance para se comunicar com agências regulatórias.

(ii) Contrapartes e clientes

Havendo um possível incidente de segurança da informação, o procedimento para comunicação com clientes e contrapartes será determinada pelo CEO e pela área de relações públicas.

8. Violações

O descumprimento de qualquer regra desta Política será considerado como falta grave, conforme disposto no Código de Conduta e Ética da EQI CTVM. A análise das violações será conduzida pela equipe de Segurança da Informação em conjunto com área de Compliance, podendo assim, aplicar sanções administrativas ao Colaborador de acordo com o grau de severidade do incidente.

9. Divulgação

A EQI CTVM se compromete, com relação a divulgação desta Política, a:

(i) Disponibilizar, sem restrições, a versão completa e atualizada da presente Política no canal de comunicação com colaboradores; e

(ii) Caso a Política sofra alteração e/ou futuras revisões, os colaboradores deverão ser comunicados através de seus veículos de comunicação internos.

10. Prazo de Validade

Após a aprovação da presente Política, ela deverá sofrer revisão anualmente ou então em período inferior, caso seja necessário tendo em vista os princípios aqui citados, assim como a legislação aplicável.

A presente Política deverá ser revisada anualmente pela área de TI.

11. Controle de Revisões

Versão	Data	Alteração	Responsável	Aprovação
1	08/12/2022	Aprovação da Política	Fabio Viana	Diretoria
2	01/09/2023	Aprovação da Política	Fabio Viana	Diretoria
3	01/06/2024	Aprovação da Política	Fabio Viana	Diretoria
4	28/01/2025	Revisão da Política	Fabio Viana	Diretoria
5	23/02/2025	Revisão da Política	Fabio Viana	Diretoria
6	26/02/2025	Revisão da Política	Fabio Viana	Diretoria
7	27/07/2025	Revisão da Política	Fabio Viana	Diretoria