Política de Segurança Cibernética da EQI CTVM

Sumário

1. Objetivo da Política 2
2. Estratégia 2
3. Estrutura da Governança de Cyber Segurança 4
4. Estrutura e Organização 5
4.1. Validação de Projetos 5
4.2. Governança 5
4.3. Identificação de Risco 6
4.4 Continuidade de Negócio 7
4.5. Monitoramento de Segurança 7
4.6. Conscientização 8
4.7. Gerenciamento de Vulnerabilidades 8
4.8. Prevenção de Ameaças Cibernéticas 9
4.9. Gestão de Identidade 9
4.10. Gestão de Terceiros 10
5. Plano de Comunicação 10
5.1. Comunicação 10
5.2. Canais de Comunicação 11
6. Divulgação 11
7. Prazo de Validade 11
8. Controle de Revisões 12

1. Objetivo da Política

A presente Política de Segurança Cibernética ("Política") tem como objetivo definir diretrizes gerais relacionadas à cyber segurança da EQI CTVM, tendo como norma relacionada a Resolução nº 4.893 do Banco Central do Brasil.

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

2. Estratégia

A cyber segurança ("Cyber Security") é um termo que determina um conjunto de tecnologias e processos que visam proteger os ativos digitais de eventuais tentativas de intrusões, danos, acessos indevidos a informações e roubo de propriedades intelectuais de uma entidade e/ou determinado grupo.

Uma estrutura de cyber segurança visa realizar tanto o monitoramento dos ativos digitais e do ambiente, através de controles e procedimentos, quanto a implementação de mecanismos para evitar que, uma vez um evento se materialize, as devidas ações sejam tomadas para minimizar os impactos aos clientes, parceiros e ao negócio da entidade.

A estratégia de defesa cibernética da EQI CTVM segue uma abordagem compreensiva de gestão de riscos e visa estabelecer o framework necessário para que a EQI CTVM:

(i) Evolua continuamente, em velocidade compatível com o desenvolvimento dos riscos e ameaças cibernéticos, aumentando a nossa resiliência a ataques e diminuindo nossas vulnerabilidades;

(ii) Reduza suas vulnerabilidades e reforce sua resiliência continuamente para antecipar a evolução do ambiente de riscos cibernéticos;

(iii) Responda com sucesso aos incidentes; e

(iv) Garanta que nosso ecossistema digital esteja seguro e resiliente.

Os objetivos da estratégia de defesa cibernética da EQI CTVM são:

(i) Identificar:

a) Em virtude das regulamentações todos os ativos de tecnologia devem ser identificados e classificados em função da sua relevância para o negócio;

b) Acompanhar a evolução dos riscos e ameaças cibernéticos para orientar e priorizar as nossas ações de defesa.

(ii) Proteger:

a) Desenvolver continuamente a cultura de segurança cibernética na EQI CTVM;

b) Reduzir nossas vulnerabilidades para assegurar que mantemos um nível adequado de segurança;

c) Proteger a confidencialidade, a integridade e a acessibilidade das informações para os colaboradores de acordo com seu escopo de trabalho.

(iii) Detectar:

a) Monitorar os ativos digitais para identificar eventos de segurança;

b) Avaliar a efetividade das nossas ações de defesa.

(iv) Responder e Recuperar:

a) Responder com eficácia a incidentes de segurança;

b) Assegurar que a EQI CTVM se recupere tempestivamente de incidentes;

c) Evoluir nossas defesas a partir das lições aprendidas com os incidentes.

A estratégia de defesa é executada segundo os seguintes princípios:

(i) Priorização de Riscos: nós devemos priorizar nossos esforços de modo a direcionar nossos recursos aos riscos de maior impacto, sejam decorrentes das maiores ameaças ou das nossas principais fraquezas;

(ii) Eficiência de Custos: nossos esforços para reforçar nossas defesas devem ser continuamente analisados para garantir que estamos obtendo os melhores resultados para cada investimento feito;

(iii) Inovação e agilidade: a evolução da tecnologia gera mais riscos, mas também gera oportunidade de inovação. Necessitamos utilizar tecnologia de ponta para reforçar nossas defesas cibernéticas e reforçar nossa agilidade na identificação e mitigação de ameaças e vulnerabilidades;

(iv) Alcance Global: Somos uma instituição com objetivos globais. Vulnerabilidades em qualquer das localidades onde podemos ter operações podem ser exploradas para atacar o grupo inteiro. Precisamos garantir que nossa estratégia de defesa cibernética é executada de forma homogênea em todas as regiões;

(v) Colaboração: Precisamos trabalhar em colaboração com todas as nossas unidades de negócio, com nossos clientes e com nossos parceiros comerciais de modo a reforçar coletivamente nossas defesas cibernéticas.

3. Estrutura da Governança de Cyber Segurança

A equipe de Segurança da Informação possui canais de comunicação direta com a alta diretoria através de diferentes fóruns e comitês estabelecidos, de forma a priorizar as ações conforme suas necessidades e sua relevância.

3.1. Comitê de Segurança da Informação (Cyber Security)

Comitê trimestral para acompanhamento dos principais projetos da área de Segurança da Informação, andamento do processo de gestão de vulnerabilidades em infraestrutura e aplicação, KPIs e relatório dos principais incidentes do mês junto com seus devidos planos de ação. Este é o principal fórum de discussão para transmitir uma visão consolidada dos principais riscos e fatores de riscos relacionados ao ambiente cibernético ao Senior Management. A partir dele, decisões estratégicas serão tomadas com o intuito de mitigar os principais riscos.

É composto pelo CEO, CTO, CIO, CFO, CRO, CISO e líderes das principais áreas de negócio de acordo com a temática.

3.2. Comitê de LGPD

Comitê semestral com a participação de representantes do Security Office, Legal, Compliance e decisores das áreas de negócios que atendem pessoas físicas para acompanhar os projetos de proteção de dados pessoais e da privacidade.

4. Estrutura e Organização

A estrutura da equipe de Segurança da Informação visa aplicar as boas práticas de mercado para que o ambiente cibernético, bem como os dados sensíveis que circulam neste meio, estejam protegidos e constantemente monitorados.

Para isso, a EQI avalia os melhores *frameworks* de mercado em relação às melhores práticas. Desta forma, a área de Segurança da Informação está segmentada em diversas frentes, conforme segue.

4.1. Validação de Projetos

Com o intuito de endereçar os principais projetos de Segurança Cibernética, elevando o nível de maturidade da instituição perante as ameaças e sua constante evolução, as seguintes atividades são elaboradas:

(i) Busca contínua por ferramentas mais modernas e robustas para o combate de ameaças;

(ii) Evolução constante dos processos e atividades realizadas pela área de Segurança da Informação (plano de ação e de resposta a incidentes, gestão de identidade, classificação de dados etc.);

(iii) Melhores práticas para a aplicação de segurança no ambiente em nuvem;

(iv) Participação nos novos projetos de TI, propondo soluções de segurança visando a confidencialidade, integridade e disponibilidade

(v) Automação de processos e atividades de Security Office.

4.2. Governança

A estrutura de Governança visa garantir a aderência da EQI CTVM em mapeamento e endereçamento dos riscos em relação às questões

regulatórias, avaliando e interpretando as demandas e traduzindo-as ao ambiente da EQI CTVM. Tem como objetivo identificar os riscos internos e externos, os ativos e processos críticos e estabelecer um conjunto de medidas cujo intuito é mitigar os riscos cibernéticos, ou seja, minimizar a probabilidade da ocorrência e da materialização de um incidente.

4.3. Identificação de Risco

O processo de Identificação de Risco visa mapear as ameaças, vulnerabilidades, fatores de riscos e analisá-los.

Uma vez identificados, define-se planos de ação para minimizar a exposição aos fatores de risco e, consequentemente, à probabilidade da ocorrência de um evento. Os processos realizados estão segregados da seguinte forma:

(i) Avaliação e identificação de riscos baseado em fatores internos e externos;

(ii) Identificação recorrente de ameaças cibernéticas em âmbito global;

(iii) Avaliação dos possíveis impactos financeiros, operacionais e reputacionais;

(iv) Definição e priorização das respostas frente aos riscos identificados;

(v) Revisão dos processos.

Por ser um processo contínuo, a etapa de revisão, executada após a definição e implementação dos planos de ação, visa avaliar se os controles que estão implementados continuam íntegros e funcionais para os riscos mapeados.

Adicionalmente, durante esta etapa, é realizado um trabalho de *follow-up* para os planos de ação em aberto, garantindo que foram implementados e incluídos na esteira de monitoramento. Além disso, o processo de Identificação de risco foca nos processos que são considerados críticos pela EQI CTVM, garantindo, assim, a integridade, confidencialidade e disponibilidade dos serviços relevantes.

4.4 Continuidade de Negócio

O processo do plano de recuperação, subprocesso de continuidade de negócio, visa simular cenários que podem causar a indisponibilidade dos processos considerados críticos para a continuidade das atividades. Os processos considerados críticos pela EQI CTVM são definidos em conjunto com os principais Heads das diversas áreas, alinhando-os à estratégia da EQI CTVM. A partir destes processos, cenários são simulados com base em ameaças que são mais propensas e factíveis de ocorrerem no ambiente da EQI CTVM e que, caso materializadas, irão causar indisponibilidade e/ou impacto relevante nestes processos. Desta forma, as pessoas chave, sistemas e suas dependências (equipamentos, serviços, outros sistemas etc.) são mapeados para que, caso a EQI CTVM enfrente um destes cenários, seja possível acionar o plano de recuperação de forma ágil e eficaz, retomando a execução dos processos considerados críticos com o menor impacto possível em sua operação.

4.5. Monitoramento de Segurança

As atividades desempenhadas pela central de monitoramento são de suma importância para resposta aos eventos e incidentes que porventura a instituição venha a sofrer.

Seguindo as boas práticas de mercado, listamos as principais atividades desempenhadas:

(i) Identificação de eventos e incidentes;
(ii) Resposta ao incidente;
(iii) Análise da exposição e riscos envolvidos;
(iv) Plano de ação;
(v) Monitoramento.

As atividades mencionadas visam, principalmente, estabelecer um fluxo em resposta aos eventos de risco e incidentes de forma tempestiva, analisando a causa-raiz, bem como a definição de planos de ação, para que o problema seja corrigido de forma definitiva. Os alertas gerados pelas ferramentas de monitoramento são classificados em diferentes níveis de

prioridade. Com isso, é possível priorizar a atuação dos esforços na análise e tratamento dos eventos.

4.6. Conscientização

Além dos riscos no mundo digital, um dos principais fatores de riscos no universo cibernético está relacionado a pessoas, sendo que grande parte dos eventos de risco que se materializam são decorrentes de falhas humanas, intencionais ou não. Assim, a EQI CTVM possui processo que visa conscientizar seus funcionários através de informes e treinamentos internos.

Desta forma, os principais processos serão:

(i) *Workshops* de conscientização aos colaboradores e, principalmente, aos novos funcionários;

(ii) Divulgação periódica de informes aos colaboradores do Grupo EQI em relação às principais vulnerabilidades que estão se materializando no mercado como um todo;

(iii) Campanhas e treinamentos relacionados às principais ameaças, incluindo campanhas específicas de *phishing*;

(iv) Treinamentos obrigatórios com periodicidade anual, visando, principalmente, reforçar a ideia e a conscientização dos principais tópicos.

4.7. Gerenciamento de Vulnerabilidades

Além das formas supracitadas, existem outras atuações visando a mitigação de vulnerabilidades, como:

(i) Aplicações de *patches* periódicos, corrigindo vulnerabilidades divulgadas pelos fornecedores e fabricantes;

(ii) Validação periódica da estrutura de *hardening* das máquinas locais e ambiente em nuvem;

(iii) Utilização de ferramentas anti-malware, IPS (Intrusion Prevention System) e IDS (Intrusion Detection System), DLP (Data Loss Prevention), análise de logs (trilhas de auditoria, logs de sistemas etc.), dentre outras;

(iv) Validação das políticas de senha dos sistemas internos, principalmente em relação aos administradores de sistemas e domínios.

4.8. Prevenção de Ameaças Cibernéticas

De forma a antever ameaças que porventura gerem incidentes e eventos de risco, a divisão de Prevenção de Ameaças Cibernéticas, realiza trabalhos preventivos com o intuito de mapear vulnerabilidades no ambiente interno e elaborar planos de ação para corrigi-las.

Posto isso, os seguintes processos são realizados:

(i) Identificação de ameaças internas e externas;

(ii) Tratativas de ataques direcionados;

(iii) Monitoramento dos principais eventos materializados no mercado e, se aplicável, implementar as devidas correções no ambiente interno;

(iv) Segurança de aplicações;

(v) Definição de baseline de segurança para novos projetos.

4.9. Gestão de Identidade

Gestão de Identidades é o processo de identificar, autenticar e autorizar os usuários e grupos de usuários aos sistemas, aplicativos e aos sistemas de armazenamento de dados de forma a garantir que o conceito de segregação de função está sendo executado.

Para garantir que funcionamento do processo, esta divisão é responsável por:

(i) Gestão de acesso aos sistemas;

(ii) Gestão de acesso aos arquivos;

(iii) Matriz de Segregação de Acesso;

(iv) Controle e gestão dos usuários que possuem privilégios (ex. administradores de máquinas, administradores de sistemas etc.).

4.10. Gestão de Terceiros

A utilização de terceiros para a execução de processos internos, algumas vezes sustentando processos críticos, necessitam de uma avaliação minuciosa em relação aos riscos em potenciais que suas operações possam gerar para a EQI CTVM. Com isso, devemos considerar cuidadosamente as melhores formas de gerenciar e minimizar a exposição a estes riscos.

A fim de manter a segurança e a gestão dos principais terceiros, o processo foi estabelecido para realizar o seguinte:

(i) Avaliação de Riscos e Planejamento;

(ii) *Due Diligence;*

(iii) Monitoramento dos Riscos e Controles.

Com base nos processos mencionados, é possível ter uma visão consolidada em relação à maturidade do ambiente de controle do prestador de serviço, tornando-se um dos critérios de avaliação em relação à continuidade e/ou contratação de determinado prestador.

5. Plano de Comunicação

Quando confirmado um incidente de segurança cibernética 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.

5.1. 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.

5.2. Canais de Comunicação

Os canais de comunicação serão estabelecidos de acordo com a disponibilidade em um eventual incidente, 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.

6. Divulgação

A EQI CTVM se compromete, com relação a divulgação dessa 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.

7. 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.

8. Controle de Revisões

Versão	Data	Alteração	Responsável	Aprovação
1	01/09/2022	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	29/01/2025	Atualização da Política	Fabio Viana	Diretoria
5	27/07/2025	Atualização da Política	Fabio Viana	Diretoria