Política de Segurança Cibernética e Segurança da Informação

Banco Capital

Versão 1.0 – maio/2019

Versão 2.0 – janeiro/2021

Versão 3.0 – setembro/2021


BANCO CAPITAL

Sumário

1. INTRODUÇÃO 4
2. OBJETIVO 4
3. ABRANGÊNCIA 4
4. PRINCÍPIOS E DEFINIÇÕES 5
5. DIRETRIZES 6
6. CLASSIFICAÇÃO DA INFORMAÇÃO 8
7. ESTRUTURA E RESPONSABILIDADES 9
7.1. Organização da Segurança da Informação 9
7.2. Comitê de Segurança da Informação 9
7.3. Comitê de Segurança Corporativa 9
7.4. Gestor Responsável pela Área 10
7.5. Responsabilidades Gerais 10
8. PROCESSOS DE SEGURANÇA DA INFORMAÇÃO 11
9. VIOLAÇÃO DA POLÍTICA E PENALIDADES 14

1. INTRODUÇÃO

A informação é o principal bem do Banco Capital e para protegê-la, a Política de Segurança Cibernética e da Informação é o documento que expressa o posicionamento da instituição em relação à proteção das suas informações e dos seus dados.

Nesse documento define-se, a estratégia de Segurança da Informação e Cyber Security a fim de proteger a integridade, disponibilidade e confidencialidade da informação, baseada na detecção, prevenção, monitoramento e resposta a incidentes e fortalece a gestão do risco de segurança cibernética e a construção de um alicerce robusto para o futuro cada vez mais digital do Banco Capital.

Para alcançarmos esse objetivo, utilizamos a estratégia de proteção de perímetro expandido. Esse conceito considera que a informação deve ser protegida independentemente de onde esteja, seja internamente, em uma coligada ou em um prestador de serviço, em todo o seu ciclo de vida, desde a coleta até o descarte.

É dever de todos seguirem as orientações contidas neste documento, bem como em todo o conjunto de normas e procedimentos que formam a matéria, para mantermos a elevada confiabilidade e credibilidade de nosso ecossistema.

2. OBJETIVO

Estabelecer os princípios, diretrizes e atribuições relacionadas à segurança da informação e privacidade, protegendo as informações da Instituição, dos clientes e do público em geral, observando as melhores práticas de mercado e regulamentações aplicáveis.

Este documento tem por objetivo orientar e definir diretrizes de condutas e responsabilidades no manuseio das informações e ativos tecnológicos do Banco Capital, visando salvaguardar seus ativos de informação, nortear a definição de normas e procedimentos específicos de Segurança da Informação, bem como implementar controles e procedimentos objetivando reduzir a vulnerabilidade da empresa a incidentes de segurança da informação, com isso garantindo a confidencialidade, integridade e disponibilidade das informações e a sua continuidade do negócio, além de proteger e manter a privacidade de dados.

A presente Política de Segurança da Informação está baseada nas recomendações da norma ABNT NBR ISO/IEC 27001, que possui as principais práticas de Segurança da Informação (SI) aplicadas mundialmente. Levou-se em conta ainda, a Resolução do Conselho Monetário Nacional (“CMN”) nº 4.893, de 26/02/2021 (“Resolução 4.893/21”) e a legislação de proteção de dados pessoais nacional, dada pela Lei nº 13.709 de 14 de agosto de 2018, também conhecida por “LGPD”.

3. ABRANGÊNCIA

As diretrizes definidas neste documento aplicam-se a todos os administradores, membros do *Board*, colaboradores, terceiros e/ou prestadores de serviço do Banco Capital, que atuem direta ou indiretamente, em nome ou benefício da Instituição, e que tenham acesso ou façam algum uso de suas informações, em qualquer meio relacionados à Instituição.

4. PRINCÍPIOS E DEFINIÇÕES

4.1. Princípios

Nosso compromisso com o tratamento adequado das informações do Banco Capital, clientes, terceiros, fornecedores e público em geral está fundamentado nos seguintes princípios:

- **Confidencialidade**: Garantia de que a informação somente estará acessível para pessoas autorizadas;
- **Integridade**: Garantia de que a informação, armazenada ou em trânsito, não sofrerá qualquer modificação não autorizada, seja esta intencional ou não;
- **Disponibilidade**: Garantia de que a informação estará disponível sempre que for necessário.

4.2. Definições

Ativos: são todos os elementos que detém algum tipo de valor para o Banco Capital. Os ativos podem ser informações, hardwares (equipamentos), softwares (sistemas) e Funcionários / Colaboradores.

BACEN: Banco Central do Brasil.

Código malicioso: termo genérico que se refere a todos os tipos de programa especificamente desenvolvidos para executar ações danosas em recursos de Tecnologia da Informação, tais como Vírus, Cavalo de Tróia, *Spyware*, *Worms*, entre outros.

Colaborador: corresponde a qualquer colaborador(a) em regime de trabalho CLT, pró-labore, estágio ou outro regime juridicamente aceito, vinculado ao Banco Capital ou a sociedade afiliada, controladora ou controlada do Banco Capital, que venha a ter acesso no exercício de suas funções a informações detidas e/ou sob o seu controle.

Custodiante: pessoa, setor ou área do Banco Capital que mantém informação sob sua guarda.

Dados pessoais: informações relacionadas diretamente a uma pessoa física identificada (ex.: número de telefone, e-mail, CPF, data de nascimento, identificadores eletrônicos), ou que podem levar à identificação de uma pessoa (ex.: GPS, redes WiFi, IDs de utilização de aplicações).

Diretoria: órgão da administração, formado pelos diretores estatutários do Banco Capital.

Incidente (de segurança): evento adverso, confirmado ou sob suspeita, motivado por violação ou falha de um controle ou procedimento de segurança, seja de forma intencional ou não, com probabilidade de colocar em risco a segurança da informação.

Informação: É um ativo que tem valor para a organização e necessita ser adequadamente protegido, independente da forma ou meio em que é apresentada. Ela pode estar impressa ou escrita em papel, armazenada eletronicamente, transmitida pelo correio ou através de meios eletrônicos, mostrada em filmes ou falada em conversas.

Gerenciamento de Risco: processo de identificação, controle e minimização ou eliminação dos riscos de segurança que podem afetar os sistemas de informação, a um custo aceitável.

LGPD: Lei nº 13.709/2018, denominada Lei Geral de Proteção de Dados, que regula o tratamento de Dados Pessoais no Brasil, em meios físicos ou digitais.

Segurança da Informação: preservação da confidencialidade, integridade e disponibilidade da informação, protegendo-a de diversos tipos de ameaças, para garantir a continuidade de negócios, minimizar perdas e danos e maximizar o retorno dos investimentos e as oportunidades de negócio.

Terceiros: entende-se tanto a entidade, quanto seu representante legal e/ou preposto que prestem ou estejam prestando serviços para a Instituição, como os prestadores de serviço em si, parceiros, franquias, fornecedores, auditores ou qualquer outro que se enquadre como prestador terceirizado.

Trilha de Auditoria: Trilha de Auditoria ou log de Auditoria trata-se de um registro de todas as ações, eventos ou atividades que um usuário ou sistema realizou com seus dados. É usada para assegurar o fluxo preciso das transações desse sistema, funcionando como complexo e detalhado rastreamento. Dessa maneira podem estar relacionados à criação, modificação, exclusão de registros ou mesmo sequência de ações automatizadas do sistema.

5. DIRETRIZES

O Banco Capital tem seus processos de segurança da informação disciplinados pelas seguintes diretrizes:

5.1. Organização da Segurança da Informação

Definir e manter uma estrutura para gerenciar a Segurança da Informação no Banco Capital.

5.2. Segurança dos Recursos Humanos

Assegurar que os colaboradores, fornecedores, e terceiros entendam seus papéis e responsabilidades, antes, durante e no encerramento ou mudança da contratação, visando reduzir o risco de roubo, fraude e mau uso de recursos e ativos de informação pertencentes ao Banco Capital.

5.3. Gestão de Ativos

Identificar e definir os controles adequados para a proteção e segurança dos ativos da empresa.

5.4. Controle de Acessos

Controlar os acessos à informação, recursos de informação e processos, com base nos requisitos de negócio e segurança da informação.

5.5. Controles Criptográficos

Assegurar o uso efetivo e adequado da criptografia para proteger a confidencialidade, autenticidade e integridade da informação.

5.6. Segurança Física

Fornecer mecanismos físicos de proteção, que abrangem desde perímetro externo até o espaço interno de trabalho, prevenindo o acesso físico não autorizado, danos, furtos e interferências com as instalações e informações críticas do Banco Capital.

5.7. Gestão das Operações e Comunicações

Garantir a operação segura e correta dos recursos de informação do Banco Capital, incluindo as atividades de rede, bem como o controle e detecção de atividades não autorizadas.

5.8. Aquisição, desenvolvimento e manutenção de sistemas

Garantir que a segurança da informação é parte integrante de todo o ciclo de vida dos sistemas de informação adquiridos, desenvolvidos e/ou mantidos pelo Banco Capital.

5.9. **Gestão de Fornecedores**

Manter um nível acordado de segurança da informação e de entrega de serviços em consonância com os acordos com fornecedores, garantindo a proteção dos ativos do Banco Capital.

5.10. **Gestão de Incidentes e Continuidade de Negócios**

Assegurar a continuidade das linhas críticas de negócio por intermédio de planos de contingência e da gestão consistente e efetiva dos incidentes de segurança da informação.

5.11. **Conformidade**

Assegurar que a segurança da informação está implementada e operada de acordo com as políticas e procedimentos da organização, evitando violação de quaisquer obrigações legais, estatutárias, regulamentares ou contratuais.

Em vistas ao cumprimento das diretrizes acima elencadas, o Banco Capital:

5.11.1. Possui como objetivo de segurança cibernética: prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados com o ambiente cibernético.

5.11.2. Com relação às medidas de segurança, adota procedimentos e controles para reduzir a vulnerabilidade da Companhia a incidentes e atender aos objetivos de segurança cibernética, dentre eles: a autenticação, a criptografia, a prevenção e a detecção de intrusão, a prevenção de vazamento de informações, a realização periódica de testes e varreduras para detecção de vulnerabilidades, a proteção contra softwares maliciosos, o estabelecimento de mecanismos de rastreabilidade, os controles de acesso e de segmentação da rede de computadores e a manutenção de cópias de segurança dos dados e das informações, conforme normativos internos vigentes.

5.11.3. Controla, monitora, restringe o acesso aos ativos de informação a menor permissão e privilégios possíveis, conforme descrito em normas internas específicas.

5.11.4. Aplica os procedimentos e controles citados anteriormente, inclusive, no desenvolvimento de sistemas de informação seguros e na adoção de novas tecnologias empregadas nas atividades da empresa.

5.11.5. Possui controles específicos, incluindo os voltados para a rastreabilidade da informação e prevenção de vazamentos, que buscam garantir a segurança das informações nos ativos, evidenciando informações sensíveis.

5.11.6. Realiza o registro, a análise da causa e do impacto, bem como o controle dos efeitos de incidentes relevantes para as atividades da empresa, que abrangem inclusive informações recebidas de empresas prestadoras de serviços a terceiros.

5.11.7. Elabora inventário dos cenários de crises cibernéticas relacionados aos incidentes de segurança considerados nos testes de continuidade de serviços financeiros prestados e testa-os anualmente para garantir a eficácia dos processos, além de produzir anualmente um relatório de resposta a incidentes no ambiente tecnológico do Banco Capital.

5.11.8. Classifica os incidentes de segurança conforme sua relevância e de acordo com (i) a classificação das informações envolvidas; e (ii) o impacto na continuidade dos negócios do Banco Capital, descritos em normas internas específicas.

5.11.9. Realiza a avaliação periódica de empresas prestadoras de serviço que realizam o tratamento de informações relevantes ao Banco Capital, com objetivo de acompanhar o nível de maturidade de seus controles de segurança para a prevenção e o devido tratamento dos incidentes.

5.11.10. Possui critérios para classificação da relevância dos serviços de processamento e armazenamento de dados e de computação em nuvem, no país ou no exterior, conforme procedimento interno.

5.11.11. Em relação à contratação de serviços relevantes de processamentos e armazenamento de dados e de computação em nuvem serão adotados os procedimentos previstos na Resolução CMN nº 4.893, de 26 de fevereiro de 2021.

5.11.12. Adota processo de gestão de continuidade de negócios relativo a segurança da informação e cibernética conforme descrito em normativo interno específico.

5.11.13. Estabelece regras e padrões para assegurar que a informação receba o nível adequado de proteção quanto à sua relevância conforme normativo interno. Toda informação possui um proprietário, é obrigatoriamente classificada e recebe os devidos controles que garantam a confidencialidade da mesma, condizendo com as boas práticas de mercado e regulamentações vigentes.

5.11.14. Realiza ações para prevenir, identificar, registrar e responder incidentes e crises de segurança que envolvam o ambiente tecnológico do Banco Capital, e que possam ocasionar o comprometimento dos pilares de segurança da informação ou gerar impacto de imagem, financeiros ou operacionais. A definição de relevância dos incidentes no ambiente tecnológico segue padrão corporativo de riscos estabelecido em norma específica.

5.11.15. Adota mecanismos para disseminação da cultura de segurança da informação e cibernética na Companhia, incluindo:

a. A implementação de programa de treinamento anual para colaboradores;
b. A prestação de informações a usuários finais sobre precauções na utilização de produtos e serviços oferecidos; e
c. O comprometimento da alta administração com a melhoria contínua dos procedimentos relacionados com a segurança da informação e cibernética.

5.11.16. Adota iniciativas para compartilhamento de informações sobre os incidentes relevantes através de filiação em fóruns de discussão.

6. CLASSIFICAÇÃO DA INFORMAÇÃO

As informações devem ser classificadas e identificadas por rótulos, considerando os seguintes níveis:

A. Pública

São informações explicitamente aprovadas por seu responsável para consulta irrestrita e cuja divulgação externa não compromete o negócio e que, por isso, não necessitam de proteção efetiva ou tratamento específico.

B. Interna

São informações disponíveis aos colaboradores para a execução de suas tarefas rotineiras, não se destinando, portanto, ao uso do público externo.

C. Confidencial

São informações de acesso restrito a um colaborador ou grupo de colaboradores. Sua revelação pode violar a privacidade de indivíduos, violar acordos de confidencialidade, dentre outros. São exemplos de informações confidenciais: dados cadastrais de colaboradores, folha salarial, dados médicos, processos judiciais.

D. Confidencial Restrita

São informações de acesso restrito a um colaborador ou grupo de colaboradores que obrigatoriamente contam como destinatários da mesma, em geral, associadas ao interesse estratégico da empresa e restritas aos gestores, presidência e funcionários cujas funções requeiram conhecê-las. São exemplos de informações confidenciais restritas: atas de reunião do

conselho com presidência e alta cúpula de gestão, indicadores e estatísticas dos processos de negócio do Banco Capital, resultado de auditorias internas.

7. ESTRUTURA E RESPONSABILIDADES

As principais responsabilidades dos colaboradores do Banco Capital, no que se referem aos processos e Política de Segurança da Informação (PSI), são:

7.1. Organização da Segurança da Informação

a. A alta direção deve apoiar ativamente e assegurar os recursos necessários à implementação da Política de Segurança Informação no Banco Capital;
b. A coordenação das atividades de segurança da informação deve ser realizada pela Área de *Compliance* e *Data Protection*, em conjunto com representantes de diferentes áreas estratégicas do Banco Capital, nas reuniões do Comitê de Segurança da Informação;
c. As responsabilidades pela segurança da informação devem estar claramente definidas e divulgadas, inclusive nos casos de terceiros;
d. O Banco Capital deve dispor de políticas de segurança que descrevam as políticas corporativas e procedimentos, estabelecendo critérios de segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações existentes;
e. As políticas e procedimentos de segurança devem ser revisados e atualizados anualmente, considerando todos os fatos e eventos relevantes que exijam, inclusive, revisão imediata.

7.2. Comitê de Segurança da Informação

a. Tem por objetivo garantir um direcionamento claro e um suporte de gestão evidente para as iniciativas de segurança do Banco Capital;
b. É composto por alguns gestores da empresa. Representantes de outras áreas poderão ser convocados para participarem de reuniões específicas;
c. É coordenado pela Área de Risco;
d. Esse Comitê reúne-se regularmente e sua frequência é de acordo com as necessidades identificadas.

7.2.1. Atribuições do Comitê de Segurança da Informação:

a. Realizar análise crítica e permanente da Política de Segurança da Informação e das responsabilidades envolvidas, deliberando sobre eventuais alterações, sempre que necessário;
b. Realizar análise crítica e monitoração dos principais riscos e incidentes de Segurança da Informação;
c. Aprovar as principiais iniciativas para aumentar o nível de Segurança da Informação;
d. Gerenciar o cumprimento da Política de Segurança do Banco Capital periodicamente, sugerindo ações que se façam necessárias;
e. Garantir a conformidade do Banco Capital com as Políticas de Segurança da Informação e suas correlatas.

7.3. Comitê de Segurança Corporativa

a. Aprimorar a qualidade e efetividade de seus processos, buscando a integridade, disponibilidade e confidencialidade das informações;

b. Proteger a informação de ameaças buscando garantir a continuidade do negócio e minimizar os riscos ao negócio;
c. Estabelecer, implementar, operar, monitorar e garantir a melhoria contínua do sistema de gestão de segurança da informação (SGSI);
d. Definir e formalizar os objetivos, controles e a estratégia de governança de segurança da informação, em conjunto com o Comitê de Segurança da Informação.
e. Coordenar as ações para atingimento dos objetivos e da estratégia de governança de segurança da informação aprovados pelos comitês, envolvendo as áreas responsáveis.
f. Estabelecer e disseminar uma cultura de segurança da informação.
g. Propor o investimento para a segurança da informação.
h. Definir as políticas e padrões de segurança da informação a serem aplicados nos processos, produtos e tecnologias.
i. Definir padrões mínimos de segurança, garantindo alinhamento com os objetivos de segurança da informação.

7.4. Gestor Responsável pela Área

a. Garantir o cumprimento desta Política e procedimentos de segurança que forem emitidos, por todos os colaboradores sob sua responsabilidade;
b. Manter as normas e os procedimentos internos da área alinhados com esta Política;
c. Divulgar a importância de sigilo de senhas, bem como o cuidado com seu uso, evitando a utilização de uma mesma senha por um grupo de colaboradores;
d. Adotar cautelas quando da admissão, transferência ou desligamento de colaboradores, a fim de evitar que documentos ou informações do Banco Capital e de seus clientes sejam usados ou divulgados indevidamente;
e. Providenciar a desativação imediata de todos os direitos de acessos de um colaborador no caso de desligamento ou de transferência para outra área;
f. Analisar periodicamente a necessidade de acessos às bases de dados e acesso a aplicativos por parte dos colaboradores sob sua responsabilidade;
g. Garantir que os contratos celebrados com outras entidades e pessoas externas ao Banco Capital (parceiros, terceiros, prestadores de serviços, fornecedores, temporários e contratados) contenham cláusulas que preservem a segurança das informações do Banco Capital, de seus clientes, parceiros e colaboradores;
h. Orientar os colaboradores que, por necessidade e natureza do trabalho, tenham de manusear ou tomar conhecimento de documentos com informações sigilosas, quanto ao zelo que devem ter com tais informações;
i. Reportar à Área de Risco as falhas e os riscos que podem levar à exposição indevida de informações críticas.

7.5. Responsabilidades Gerais

a) Todas as informações trocadas ou armazenadas nos ativos de informação do Banco Capital, independentemente de conteúdo, são de propriedade única e exclusiva da instituição. Os colaboradores devem utilizar os recursos disponibilizados pelo Banco Capital para a condução dos negócios da instituição;
b) Compete a todos os colaboradores o cumprimento das diretrizes constantes desta Política e das demais políticas de Segurança da Informação, bem como do Código de Ética e Conduta e Política de Privacidade do Banco Capital;

c) Os colaboradores do Banco Capital devem comunicar formalmente ao Comitê de Segurança da Informação quaisquer irregularidades ou desvios relativos à Segurança da Informação identificados;
d) Todo colaborador deve aderir formalmente ao Contrato de Segurança e Termo de Responsabilidade e Confidencialidade.

8. PROCESSOS DE SEGURANÇA DA INFORMAÇÃO

Para assegurar que as informações tratadas estejam adequadamente protegidas, o Banco Capital adota os seguintes processos:

a. Gestão de Ativos

Entende-se por ativo, tudo aquilo que a instituição considerar como relevante para o negócio, desde ativos tecnológicos (p.ex. *software* e *hardware*), como não tecnológicos (p.ex. pessoas, processos e dependências físicas) desde que estejam relacionados à proteção da informação. Os ativos, de acordo com sua criticidade, devem ser identificados, inventariados, mantidos atualizados e serem protegidos contra acessos indevidos. A proteção pode ser: física (p.ex. salas com acesso controlado) e lógica (p.ex. configurações de blindagem ou *hardening*, *patch management*, autenticação e autorização). Os ativos do Banco Capital, dos clientes e do público em geral devem ser tratados de forma ética e sigilosa e de acordo com as leis vigentes e normas internas, promovendo o uso adequado e prevenindo exposição indevida das informações.

b. Classificação da Informação

Para classificação das informações devem ser consideradas as necessidades relacionadas ao negócio, o compartilhamento ou restrição de acesso e os impactos no caso de utilização indevida das informações. De acordo com a classificação da confidencialidade devem ser estabelecidas as proteções necessárias durante todo o seu ciclo de vida.

O ciclo de vida da informação compreende: Geração, Manuseio, Armazenamento, Transporte e Descarte.

c. Gestão de Acessos

As concessões, revisões e exclusões de acesso devem utilizar as ferramentas e os processos corporativos do Banco Capital. Os acessos devem ser rastreáveis, a fim de permitir a identificação individual do colaborador ou prestador de serviço que tenha acessado ou alterado as informações, permitindo sua responsabilização. A concessão de acessos deve obedecer ao critério de menor privilégio, no qual os usuários devem ter acesso somente aos recursos de informação imprescindíveis para o pleno desempenho de suas atividades e devidamente autorizados. A segregação de funções deve permear todos os processos críticos, evitando que um único responsável possa executar e controlar o processo durante todo seu ciclo de vida. A identificação de qualquer colaborador deve ser única, pessoal e intransferível, qualificando-o como responsável pelas ações realizadas.

A senha é uma informação confidencial, pessoal e intransferível, deve ser utilizada como assinatura eletrônica, sendo proibido seu compartilhamento.

d. Gestão de Riscos

Os riscos devem ser identificados por meio de um processo estabelecido para análise de ameaças, vulnerabilidades, probabilidades e impactos sobre os ativos do Banco Capital, para que sejam recomendadas as proteções adequadas. As recomendações são discutidas nas reuniões apropriadas pelo Comitê de Segurança da Informação. Produtos, processos e

tecnologias devem ter a adequada gestão dos riscos de Segurança da Informação, para redução dos riscos a níveis aceitáveis, independentemente de estarem dentro da infraestrutura do Banco Capital, parceiros ou prestadores de serviços. As tecnologias em uso pela instituição devem estar em versões suportadas pelos seus fabricantes e devidamente atualizadas. Eventuais exceções devem ser aprovadas na alçada competente ou possuir controles compensatórios.

e. Gestão de Riscos em Prestadores de Serviços

Os prestadores de serviços contratados pelo banco devem ser classificados considerando alguns critérios. Dependendo da classificação, o prestador de serviços passará por avaliação de risco, que pode incluir a validação *in loco* dos controles de Segurança da Informação, avaliação remota das evidências ou outras avaliações, além do acompanhamento de eventuais correções e melhorias implementadas pelos prestadores de serviços. Os prestadores de serviços devem informar os incidentes relevantes, relacionados às informações do Banco Capital armazenadas ou processadas por eles em cumprimento às determinações legais e regulamentares.

f. Tratamento de Incidentes de Segurança da Informação e Cyber Security

A área de Tecnologia da Informação monitora a segurança do ambiente tecnológico do Banco Capital, analisando os eventos e alertas para identificar possíveis incidentes. Os incidentes que são identificados pelos alertas são classificados com relação ao impacto, de acordo com os critérios adotados pelo Banco Capital. 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. Incidentes classificados como relevantes devem ser comunicados, de imediato, ao Comitê de Segurança da Informação. Informações sobre incidentes que possam impactar outras instituições financeiras no Brasil, devem ser compartilhadas com as demais instituições, visando colaborar com a mitigação do risco conforme determinações legais e regulamentares. A área de Riscos elaborará um Relatório Anual contendo os incidentes relevantes ocorridos no período, ações realizadas de prevenção e resposta aos incidentes. Este relatório deverá ser apresentado ao Comitê de Segurança da Informação e à Diretoria, conforme determinações legais e regulamentares. Todo colaborador deve ser proativo e diligente na identificação, comunicação para a área de Segurança da Informação e área de Riscos e na mitigação dos riscos relacionados à Segurança da Informação.

g. Conscientização em Segurança da Informação e Cyber Security

O Banco Capital promove a disseminação dos princípios e diretrizes de Segurança da Informação por meio de conscientização e capacitação de colaboradores, terceiros e demais envolvidos no tratamento e acesso a informações, para fortalecer a cultura de Segurança da Informação.

h. Governança com as Áreas de Negócio e Tecnologia

As iniciativas e projetos das áreas de negócio e tecnologia devem estar alinhadas com os princípios e diretrizes de Segurança da Informação.

i. Segurança Física do Ambiente

O processo de segurança física estabelece controles relacionados à concessão de acesso físico aos ambientes, de acordo com a criticidade das informações tratadas nestes ambientes. O Banco Capital deve implementar sistema para controle de acesso dos Colaboradores, prestadores de serviços, fornecedores, provedores e parceiros aos locais restritos. Os equipamentos e instalações de processamento de informação crítica ou sensível devem ser mantidos em áreas

seguras, com níveis de controle de acesso apropriados, incluindo proteção contra ameaças físicas e ambientais.

j. Segurança no Desenvolvimento de Sistemas de Aplicação

O processo de desenvolvimento de sistemas deve garantir a aderência aos normativos externos e internos e boas práticas de segurança da instituição. Todo o ciclo de vida do desenvolvimento dos softwares do Banco Capital deve seguir as melhores práticas de desenvolvimento a fim de produzir *softwares* seguros, buscando mitigar o surgimento de vulnerabilidades relacionadas à segurança. Todo desenvolvimento ou manutenção de *software* devem ser formalmente autorizados e deve ser realizada uma análise de impacto. Todas as ferramentas de desenvolvimento devem ser homologadas e licenciadas. O projeto de *software* deve conter um documento de especificação de segurança que descreva seus objetivos de segurança.

k. 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. Essas informações devem ser protegidas contra modificações e acessos não autorizados. Todas as transações relacionadas aos clientes devem gerar trilhas de auditoria (*logs*), que deverão ser mantidas de acordo com as legislações vigentes, protegido contra acessos não autorizados. Não deve haver nenhuma modificação na integridade das trilhas de auditoria (*logs*), sendo assim, não pode haver usuários com permissão de alteração nesses registros.

l. Programa de *Cyber Security*

O Programa de *Cyber Security* do Banco Capital é norteado pelos seguintes fatores:

- Regulamentações vigentes;
- Melhores práticas;
- Cenários mundiais;
- Análises de risco da própria instituição, conforme sua criticidade, as ações do programa dividem-se em:
    - Críticas: Consiste de correções emergenciais e imediatas para mitigar riscos iminentes;
    - Sustentação: Iniciativas de curto/médio prazo, para mitigação de risco no ambiente atual, mantendo o ambiente seguro, respeitando o apetite de risco da instituição e permitindo que ações de longo prazo/estruturantes possam ser realizadas;
    - Estruturantes: Iniciativas de médio/longo prazo que tratam a causa raiz dos riscos e que preparam o banco para o futuro.

m. Proteção de perímetro

Para proteção da infraestrutura do Banco Capital contra um ataque externo, utilizamos, no mínimo, ferramentas e controles contra: ataques de *DDoS*, *Spam*, *Phishing*, *Ransonware*, *APT/Malware*, invasão de dispositivos de rede e servidores, ataques a aplicação e *scan* externos. Para mitigação do risco de vazamento de informações utilizamos ferramentas preventivas instaladas nos servidores, estações de trabalho, no serviço de correio eletrônico, no serviço de navegação *WEB*, além do uso de criptografia para dados em repouso e em transporte. Visando elevar a proteção, não é permitida a conexão física ou lógica à rede corporativa da instituição, por equipamentos particulares ou não homologados pelo setor de Tecnologia da Informação.

n. Testes de varredura para detecção de vulnerabilidade

O Banco Capital possui processo para identificar e eliminar as vulnerabilidades de seus sistemas, rede e servidores, para assegurar a integridade do ambiente dos processos de negócio. Para tanto, deve promover monitoramento constante e condução de testes e varredura para detecção de vulnerabilidades, avaliação de riscos e determinação de medidas de correção adequadas. As vulnerabilidades identificadas devem ser tratadas e priorizadas de acordo com seu nível de criticidade.

A Equipe de Segurança da Informação deverá acompanhar todo o processo a fim de obter informações necessárias para realização de uma gestão sobre as aplicações de correções de vulnerabilidade, essas informações alimentará o controle de Segurança da Informação para as vulnerabilidades do ambiente do Banco Capital.

o. Propriedade Intelectual

A propriedade intelectual é a proteção que recai sobre bens imateriais, tais como: marcas, sinais distintivos, *slogans* publicitários, nomes de domínio, nomes empresariais, indicações geográficas, desenhos industriais, patentes de invenção e de modelo de utilidade, obras intelectuais (tais como obras literárias, artísticas e científicas, base de dados, fotografias, desenhos, ilustrações, projetos de arquitetura, obras musicais, obras audiovisuais, textos e etc.), programas de computador e segredos empresariais (inclusive segredos de indústria e comércio). Pertencem exclusivamente ao Banco Capital todas e quaisquer invenções, criações, obras e aperfeiçoamentos que tenham sido ou venham a ser criados ou realizados pelo colaborador ao Banco Capital, na qualidade de administrador, empregado e/ou estagiário, durante todo o prazo de vigência do mandato, contrato de trabalho ou contrato de estágio do colaborador. Quaisquer informações e conteúdos cuja propriedade intelectual pertença ao Banco Capital, ou tenham sido por ele disponibilizado, inclusive informações e conteúdos que tenham sido obtidos, inferidos ou desenvolvidos pelo próprio colaborador em seu ambiente de trabalho ou utilizando recursos da instituição não devem ser utilizados para fins particulares, nem repassados a terceiros, sem autorização prévia e expressa do Banco Capital. É dever de todos os colaboradores zelar pela proteção da propriedade intelectual do Banco Capital.

p. Declaração de Responsabilidade

Periodicamente os colaboradores do Banco Capital devem aderir formalmente a um termo, comprometendo-se a agir de acordo com as políticas de Segurança da Informação. Os contratos firmados com o Banco Capital devem possuir cláusula que assegure a confidencialidade e privacidade das informações tratadas.

9. VIOLAÇÃO DA POLÍTICA E PENALIDADES

A não observância dos princípios e diretrizes constantes nesta Política pode impactar seriamente os clientes do Banco Capital, possibilitar a violação de leis e regulamentos, e afetar negativamente a reputação e a estabilidade financeira da empresa. Desvios e exceções devem ser tratados pelo Comitê de Segurança da Informação.

Colaboradores, fornecedores ou outros *stakeholders* que observarem quaisquer desvios às diretrizes desta política poderão relatar o fato ao Canal de Ética do Banco Capital (compliance@socialbank.com.br), podendo ou não se identificar. Internamente, o descumprimento das diretrizes desta Política enseja a aplicação de medidas de responsabilização dos agentes que a descumprirem, conforme a gravidade do descumprimento.

Salvador, 15 de setembro de 2021.

_____

Alvaro Henrique Guimarães da Paixão

Setor TI

Assinatura Diretores:

_____ _____

Angelo Augusto Viana da Silveira

Ana Maria da Cunha Guedes Rêgo