FRAM CAPITAL

FRAM Capital
Gestão de Ativos

Política de Segurança da Informação e Cibernética

Agosto | 2025

FRAM CAPITAL

SUMÁRIO

1. OBJETIVO

1.1. A informação é um dos principais bens de toda organização. O fluxo e uso adequado da informação é essencial para o funcionamento eficiente da organização, bem como o gerenciamento dos riscos e ameaças inerentes à crescente facilidade de acesso à informação. Um dos objetivos da presente Política de Segurança da Informação e Cibernética ("Política") é a mitigação de eventuais vulnerabilidades e ameaças à segurança da informação na FRAM Capital Gestão de Ativos Ltda. ("FRAM Capital"), por meio da definição de mecanismos de prevenção, detecção e mitigação de incidentes de segurança da informação ou relacionados ao ambiente cibernético.

1.2. A FRAM Capital estabelece diretrizes que compõem um programa completo e consistente de segurança da informação e riscos cibernéticos, visando:

a) a proteção do valor e da reputação da FRAM Capital;

b) a garantia da confidencialidade, integridade e disponibilidade das informações próprias e de terceiros por ele custodiadas, contra acessos indevidos e modificações não autorizadas, assegurando, ainda, que as informações estejam disponíveis às partes autorizadas, quando necessário;

c) a identificação de incidentes de segurança cibernética, ameaças e vulnerabilidades, estabelecendo ações sistemáticas de detecção, tratamento e prevenção, objetivando a mitigação dos riscos cibernéticos, dentre outros;

d) a garantia da continuidade de seus negócios, mitigando a probabilidade da ocorrência de interrupções decorrentes de falhas relacionadas à segurança da informação ou cibernética;

e) conscientização, educação e treinamento de todos os sócios, diretores, membros da alta administração e dos órgãos de governança, administradores, empregados, prestadores de serviço e colaboradores da FRAM Capital ("Colaboradores") da FRAM Capital;

f) estabelecer e melhorar continuamente o processo de gestão de riscos de segurança cibernética;

g) a confiabilidade e adequação de todas as informações sob gestão da área de Tecnologia da Informação, assegurando a proteção de todos os ativos, dados, programas e equipamentos; e

h) a administração da concessão de acessos a sistemas, dados e serviços.

2. BASE NORMATIVA[1]

2.1. A presente Política foi elaborada com base nas seguintes normas:

Lei Federal nº 13.709, de 14 de agosto de 2018

Resolução nº 175, de 23 de agosto de 2022, da Comissão de Valores Mobiliários

[1] Todas as referências às disposições legais ou regulamentares devem ser interpretadas como referências às disposições em vigor, conforme respectivamente alteradas, estendidas, consolidadas ou reformuladas.

Guia de Cibersegurança da Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais (ANBIMA)

3. ABRANGÊNCIA

3.1. Esta Política se estende a todos os Colaboradores, que devem pautar a sua conduta em conformidade com os princípios gerais e regras aqui estabelecidos. Esta Política é revisada com o suporte da área de Tecnologia da Informação e é divulgada aos Colaboradores.

3.2. A utilização dos recursos de tecnologia da informação é monitorada, com a finalidade de detectar eventuais não conformidades com a presente Política. A gestão de incidentes de segurança da informação está sob responsabilidade do *Data Protection Officer* ("DPO").

4. ESTRUTURA DE GOVERNANÇA

4.1. A Diretoria Executiva é o órgão máximo de deliberação da FRAM Capital e tem atuação pautada pelo comprometimento da FRAM Capital com as melhores práticas na governança e no processo de segurança da informação, melhorando continuamente esta Política e promovendo a cultura organizacional sobre este assunto. Nesse sentido, são atribuições da Diretoria Executiva:

a) estabelecer e revisar as diretrizes da Política de Segurança da Informação, no mínimo, anualmente;

b) prover recursos para que os Colaboradores possam alcançar seus objetivos;

c) zelar pela prevenção de incidentes relacionados à segurança da informação;

d) avaliar a efetividade desta Política e dos procedimentos relacionados à segurança da informação;

a) incentivar continuamente a disseminação de uma cultura de gestão de riscos; e

b) manter Colaboradores experientes, qualificados, motivados, continuamente treinados e comprometidos com suas atribuições e responsabilidades.

4.2. São atribuições do Comitê de Riscos e Compliance:

a) aprovar os manuais de procedimentos que envolvem segurança da informação;

d) analisar as demandas levadas às reuniões do Comitê de Riscos e *Compliance,* emitindo pareceres e decisões de acordo com esta Política e com a legislação aplicável; e

e) zelar pelos manuais que envolvem segurança da informação, descritos neste documento.

4.3. São atribuições da área de Tecnologia da Informação:

a) a manutenção contínua do ambiente tecnológico seguro e que suporte a operação da FRAM Capital;

b) oferecer suporte técnico e operacional às demais áreas nos assuntos relacionados à

segurança da informação; e

c) manter seus processos aderentes às disposições desta Política.

4.4. São atribuições da área de Compliance:

a) divulgar e dar conhecimento a todos os Colaboradores sobre as normas e os procedimentos relativos à segurança da informação;

b) orientar todos os Colaboradores de acordo com as regras estabelecidas nesta Política;

c) promover adequado treinamento dos Colaboradores; e

d) executar rotinas de diligência sobre a aderência dos processos da FRAM Capital às diretrizes da presente Política.

4.5. Por fim, é atribuição da área de Riscos e Compliance realizar testes, mapear falhas e conduzir planos de ação para eventual correção que se faça necessária, em conjunto, conforme o caso, à área de Tecnologia da Informação.

5. SEGURANÇA DA INFORMAÇÃO

5.1. Os gestores de cada equipe são responsáveis pela aderência dos membros de seus times a esta Política. Os Colaboradores que compõem a área de Tecnologia da Informação são responsáveis pelos procedimentos de segurança dos equipamentos e acessos.

5.2. Através da equipe de Tecnologia da Informação, a FRAM Capital efetua avaliações de risco regulares do ambiente de segurança da informação, para identificar potenciais vulnerabilidades e garantir que as medidas de segurança reduzem e mitigam os riscos e suprem patamares apropriados. Os riscos da referida avaliação interna incluem:

a) a identificação do nível de acesso de cada usuário;

b) a garantia da segurança de cada terminal e dos materiais impressos em nome da FRAM Capital;

c) a detecção do uso da internet ou de aplicativos que permitam invasão;

d) a detecção de mensagens eletrônicas forjadas, como *Phishing*; e

e) o uso de credenciais e o acesso de terceiros.

5.3. O compromisso da FRAM Capital com o tratamento adequado das informações está fundamentado nos seguintes princípios:

a) confidencialidade – o acesso à informação é obtido somente por pessoas autorizadas e quando necessário;

b) disponibilidade – as pessoas autorizadas têm acesso à informação, sempre que necessário;

c) integridade – a exatidão e a completude da informação e dos métodos de seu processamento;

d) confiabilidade – a transparência no tratamento e na interação com os públicos

envolvidos;

e) **segurança** – utilização de medidas técnicas e administrativas aptas a proteger os dados de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

f) **prevenção** – adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados; e

g) **prestação de contas** – demonstração da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento desta Política e da Política de Privacidade e Proteção de Dados Pessoais e, inclusive, da eficácia dessas medidas.

5.4. Esta Política se aplica a todas as informações tratadas pela FRAM Capital, incluindo, mas não se limitando àquelas:

a) escritas em papel;

b) armazenadas ou transmitidas por meios eletrônicos; e

c) trocadas em conversas formais e informais.

5.5. Independentemente da forma ou do meio pelo qual a informação for apresentada ou compartilhada, sempre deverá estar protegida adequadamente, de acordo com controles definidos nesta Política. Todos os usuários que utilizam Sistemas de Informação da FRAM Capital devem, obrigatoriamente, conhecer e cumprir esta Política. Caso algum usuário perceba qualquer incidente de segurança da informação, deve informar o ocorrido imediatamente às áreas de *Compliance* e Tecnologia da Informação.

5.6. As informações de propriedade da FRAM Capital devem ser utilizadas apenas para atender as finalidades descritas nas políticas internas da instituição, em linha com os seus melhores interesses. Os usuários não podem, em nenhuma hipótese, apropriar-se dessas informações ou exportá-las, independentemente do meio utilizado, tais como CDs, *pendrives*, cartões de memória, ou qualquer outra mídia de armazenamento de dados. Todos os documentos produzidos por qualquer Sistema de Informação da FRAM Capital são de propriedade exclusiva desta instituição.

5.7. O usuário de rede, com acesso por meio de senha, é pessoal e intransferível, qualificando o Colaborador em questão como responsável por todas as atividades desenvolvidas ou praticadas por meio do respectivo usuário. Portanto, a senha é de uso pessoal e intransferível, não devendo ser compartilhada com terceiros, incluindo, mas não se limitando a, outros Colaboradores.

5.8. A FRAM Capital, por meio de suas áreas de *Compliance* e Tecnologia da Informação, reserva-se o direito de monitorar o tráfego de seus Colaboradores nos Sistemas de Informação da FRAM Capital, incluindo o acesso à internet e o uso do correio eletrônico, em a conformidade com as normas e procedimentos descritos nesta Política.

5.9. As informações restritas e confidenciais têm classificação de segurança, para que haja proteção adequada quanto ao seu acesso e uso.

5.10. A informação deve receber proteção adequada em observância aos princípios e diretrizes de segurança da informação da FRAM Capital em todo o seu ciclo de vida, que compreende:

a) geração;
b) manuseio;
c) armazenamento;
d) transferência;
e) transporte; e
f) descarte.

5.11. O acesso a Sistemas de Informação, incluindo plataformas e equipamentos, é disponibilizado pela FRAM Capital aos determinados Colaboradores. Não é permitido o compartilhamento com terceiros e o uso em não conformidade com os objetivos corporativos ou com esta Política.

5.12. A FRAM Capital tem o direito irrestrito, independentemente de qualquer aviso prévio, notificação ou formalidade, de inspecionar quaisquer dados contidos nos equipamentos, na rede e nos demais Sistemas de Informação se sua propriedade ou a ela licenciados, para prevenir, detectar ou mitigar o seu uso inadequado.

5.13. Para assegurar que as informações tratadas estejam adequadamente protegidas, a FRAM Capital adota as diretrizes descritas abaixo.

a) Gestão de ativos da informação: entende-se por ativos da informação tudo o que pode criar, processar, armazenar, transmitir e excluir informação, tecnológicos, tais como *software* e *hardware*, ou não tecnológicos, tais como pessoas e dependências físicas. Os ativos devem ser identificados de forma individual, inventariados e protegidos de acessos indevidos. Alguns métodos de proteção e segurança são aplicados aos ativos da informação para protegê-los contra acessos indevidos ou não autorizados, advindos de meio externo ou interno, tais como dispositivos móveis (*pendrives*, cartões de memória, HD externo ou equivalentes) ou mídias removíveis (*smartphones*, câmeras, gravadores e equivalentes). Os equipamentos pertencentes à FRAM Capital de uso individual ou coletivo, os servidores de dados e os aplicativos estão dotados de mecanismos de proteção contra vírus e *malwares*.

b) Transferência de dados: a FRAM Capital estabelece diretrizes e padrões para os procedimentos de transferência de dados, interna e externamente, com proteção e segurança, por meio de análises e investigação de vulnerabilidades nos recursos de processamento da informação, permitindo correções e adequações tempestivas, minimizando os riscos de violação de dados e de vazamento de dados.

5.14. Os dados devem ser classificados de acordo com a sua confidencialidade e as proteções necessárias, nos seguintes níveis:

a) **Informação Restrita**: toda e qualquer informação associada aos interesses estratégicos da FRAM Capital, de posse da diretoria, dos comitês e dos gestores das áreas. O acesso a esse tipo de informação deve ser limitado a um número reduzido de pessoas autorizadas e, se revelada ou adulterada, pode trazer sérios prejuízos à instituição e gerar impactos negativos nos negócios e à imagem da FRAM Capital ou de seus Colaboradores. Essas informações requerem medidas de controle e proteção rigorosas contra acessos, cópias ou reproduções não autorizadas. Em geral, seu acesso é limitado à diretoria, gerentes das áreas, jurídico e Colaboradores previamente designados.

b) **Informação Confidencial**: informação transmitida por qualquer meio, cujo conhecimento está limitado a Colaboradores que dela necessitem saber ou ter acesso para o exercício de sua função na FRAM Capital. A divulgação ou adulteração desse tipo de informação pode trazer impactos negativos aos negócios da FRAM Capital e à gestão de processos, bem como prejuízos à imagem da FRAM Capital ou de seus Colaboradores.

c) **Informação de Uso Interno**: toda informação cujo conhecimento e uso estão restritos ao ambiente interno e aos propósitos da FRAM Capital, estando disponível aos Colaboradores e podendo ser revelada ao público externo apenas mediante autorização do gestor da informação.

d) **Informação de Uso Público**: toda informação que pode ser divulgada para o público externo à FRAM Capital, sem implicações de proteção e controle de acesso.

5.15. Caso um Colaborador tenha acesso à determinada informação sem autorização prévia, este deverá, imediatamente, abster-se de usar tal informação em seu benefício, em benefício de clientes da FRAM Capital ou em benefício de terceiros, devendo informar a o time de *Compliance* acerca do ocorrido. A FRAM Capital veda expressamente aos Colaboradores efetuar qualquer tipo de operação no mercado financeiro ou de capitais baseada em informações privilegiadas, bem como recomendá-las ou sugeri-las a terceiros. Ressalta-se que a realização de operações com o uso de informações privilegiadas fere esta Política, a lei e as normas aplicáveis à FRAM Capital, podendo geral responsabilização nas esferas cível e criminal.

5.16. Todas as Informações Confidenciais recebidas devem ser analisadas pelo Colaborador atentamente, principalmente, mas não limitado a, em caso de identificação das situações descritas abaixo.

a) compra ou venda de títulos e valores mobiliários por meio do uso de informação privilegiada, com a intenção de auferir benefício para si ou para terceiros;

b) compra ou venda de títulos e valores mobiliários de forma a concluir ou obter vantagem econômica antecipadamente a outros; e

c) qualquer outra prática que não esteja alinhada aos interesses da FRAM Capital e de

seus clientes.

5.17. Na classificação de um conjunto de informações que apresente diversos níveis de confidencialidade, deve-se adotar a classificação de maior nível presente no conjunto. Para isso, devem ser consideradas as necessidades relacionadas aos negócios, o compartilhamento ou restrição de acesso e os impactos no caso de utilização indevida ou divulgação não autorizada das informações. Tal classificação deve ser atribuída pelo gestor da informação e deve ser mantida durante o seu tratamento.

5.18. Para que não restem dúvidas, consideram-se privilegiadas todas as informações às quais o Colaborador tenha acesso em razão do exercício de suas funções na FRAM Capital.

6. SEGURANÇA CIBERNÉTICA

6.1. O programa de segurança cibernética da FRAM Capital é norteado pelas seguintes diretrizes.

a) **Identificação e avaliação de riscos (*risk assessment*)** – identificação dos riscos internos e externos. A mensuração dos riscos se dá por meio do mapeamento dos Sistemas de Informação da FRAM Capital ou utilizados pela FRAM Capital que contêm Informações Restritas, para protegê-los de forma adequada.

b) **Ações de prevenção e proteção** – estabelecimento de um conjunto de medidas cujo objetivo é mitigar e minimizar a concretização dos riscos identificados no item anterior, por meio da programação e implementação de controles. As ações de prevenção adotadas pela FRAM Capital incluem: utilização e atualização de sistemas antivírus, instauração de DLP, para a prevenção de desvios e perda de arquivos, execução de testes e reporte obrigatório de phishing.

c) **Monitoramento e testes** – detecção de ameaças em tempo hábil, de forma a reforçar os controles, caso necessário, e de anomalias no ambiente tecnológico, incluindo a presença de usuários, componentes ou dispositivos não autorizados. A FRAM Capital realiza monitoramento, em todo o ambiente cibernético existente, de forma física e em nuvem. Dessa forma, caso ocorram falhas, perdas ou inconsistências, as áreas de Tecnologia da Informação e *Compliance* são imediatamente acionadas. A FRAM Capital também conduz testes de funcionamento dos Sistemas de Informação por ela disponibilizados, por meio de sua equipe da Tecnologia da Informação.

d) **Adoção de plano de resposta a incidentes** – a FRAM Capital adota um plano de resposta e tratamento de incidentes de segurança da informação, que inclui a comunicação interna e, conforme o caso, externa. .

e) **Governança** – manutenção do programa de segurança cibernética continuamente atualizado, garantindo que ações, processos e indicadores sejam regularmente executados.

6.2. Conforme sua criticidade, as ações do programa de segurança cibernética dividem-se

em:

a) ações críticas: correções emergenciais e imediatas para mitigar riscos iminentes;

b) ações de sustentação: iniciativas de curto ou médio prazo, para mitigação de risco no ambiente atual, mantendo o ambiente seguro, respeitando o apetite ao risco da FRAM Capital e permitindo que ações de longo prazo ou estruturantes possam ser implementadas; e

c) ações estruturantes: iniciativas de médio a longo prazo que tratam a causa raiz dos riscos e que preparam a FRAM Capital para o futuro.

6.3. A FRAM Capital conta com *Firewall* em balanceamento com dois *links* para disponibilidade dos serviços para a infraestrutura e tráfego, trabalhando com segmentação da rede. A rede Wi-Fi fica isolada da rede local por segurança e o acesso às dependências físicas da FRAM Capital é controlado por biometria. Todos os ativos da FRAM Capital e o tráfego das informações tratadas pela instituição ou por seus Colaboradores são gerenciados e monitorados de forma centralizada pela área de Tecnologia da Informação.

7. SEGURANÇA FÍSICA DO AMBIENTE

7.1. A segurança física do ambiente refere-se às medidas de segurança adotadas no ambiente físico da FRAM Capital. A segurança física visa à proteção de dados sensíveis contra acesso não autorizado, modificação ou destruição, assim como à proteção do próprio sistema de tecnologia da informação contra o uso não autorizado ou danos físicos.

7.2. O processo de segurança física estabelece controles relacionados à concessão de acesso às instalações da FRAM Capital somente a pessoas autorizadas e previamente identificadas. Uma das formas de proteção das instalações da FRAM Capital é o estabelecimento de perímetros de segurança física. Assim, a FRAM Capital possui instalações de acesso restrito a pessoas autorizadas, por meio de reconhecimento facial. A FRAM Capital também registra os acessos às referidas instalações.

8. NORMAS DE UTILIZAÇÃO

a) Internet

8.1. O acesso à internet na FRAM Capital é uma concessão feita aos usuários, e não um direito. O usuário deve utilizá-la somente para atividades ligadas ao exercício de sua função. Os usuários devem utilizar a internet de forma adequada e diligente, em conformidade com a lei, a moral e a ordem pública, abstendo-se da prática de atos ilícitos, lesivos aos direitos e interesses da FRAM Capital ou que, de qualquer forma, possam danificar, inutilizar, sobrecarregar ou deteriorar os recursos tecnológicos e documentos da FRAM Capital.

8.2. É proibida a divulgação ou o compartilhamento não autorizados de informações

sigilosas em listas de discussão, bate-papo ou *softwares* de mensagens eletrônicas. Usuários com acesso à internet não podem efetuar *upload* de *softwares* ou dados cuja licença ou propriedade pertençam à FRAM Capital. A exceção a tais disposições, em casos especiais, é tratada internamente, mediante autorização do(s) gestor(es) responsável(is) pelo(s) *software*(s) ou dado(s).

8.3. *Downloads* são autorizados, desde que a fonte seja confiável. Contudo, para a instalação de softwares oriundos da Internet, é necessária autorização prévia da área de Riscos e Compliance.

8.4. Cada usuário é responsável por zelar pelo cumprimento desta Política e de todas as atividades realizadas por intermédio de seu usuário de rede. Não é permitida a utilização de *software peer-to-peer*, o acesso a sites de relacionamento (como Facebook, "X", Instagram e afins) e congêneres.

b) Meios de Comunicação Informais

8.5. De acordo com a regulamentação aplicável, as ligações telefônicas e mensagens instantâneas em nome da FRAM Capital são registradas, monitoradas e armazenadas. Os Colaboradores estão cientes do sistema de gravação telefônica e de mensagens instantâneas e, por isso, concordam que os usos de meios de comunicação são monitorados, não sendo reservado ao Colaborador nenhum direito sobre o material coletado.

c) Correio Eletrônico

8.6. Por ser uma ferramenta de trabalho, as contas de correio eletrônico têm titularidade única e exclusiva, o que determina a responsabilidade direta do usuário. As contas de serviço, por sua vez, possuem um ou mais responsáveis pelo seu uso. A utilização do correio deve ser feita de forma adequada e diligente, sendo vedada, a todos os usuários, a utilização do correio eletrônico para as seguintes atividades:

a) envio de mensagens não autorizadas, divulgando informações sigilosas;

b) acesso não autorizado à caixa postal de outro usuário ou de serviços;

c) envio, manuseio e armazenamento de material que caracterize a divulgação, incentivo ou prática de atos ilícitos, proibidos, contrários aos direitos e interesses da FRAM Capital, que possam danificar, inutilizar, sobrecarregar ou deteriorar *hardware* ou *software*, documentos e arquivos de qualquer tipo, ou que contrariem a moral, os bons costumes e a ordem pública;

d) envio de mensagens do tipo "corrente", "spam" ou que contenham vírus eletrônico ou qualquer forma de programação (arquivos executáveis ou do tipo *script*) que sejam prejudiciais ou danosas aos destinatários das mensagens;

e) utilização de listas ou caderno de endereços para distribuição de mensagens que não

tenham relação com os interesses da FRAM Capital ou a devida permissão do responsável pelas listas ou caderno de endereços em questão; e

f) todo e qualquer uso do correio eletrônico não previsto nesta Política que afete a FRAM Capital de forma negativa.

d) Contas e Senhas

8.7. Com o intuito de controlar a concessão de acessos a Sistemas de Informação, a FRAM Capital estabelece as normas abaixo, para evitar o uso inapropriado de senhas. Ressalta-se que todas as senhas de rede são pessoais e intransferíveis, devendo ser mantidas em sigilo, e cada usuário é responsável por sua senha, sendo responsabilizado pelo mau uso desta.

Senha de rede - os usuários devem estabelecer senhas de acesso ao *notebook* ou ao *desktop*, de seis a oito caracteres, sendo obrigatório o uso de letras maiúsculas e minúsculas, números e caracteres especiais (@%^; ou espaço). Na ocorrência de várias tentativas frustradas de ingresso por erro no fornecimento da senha, o usuário é bloqueado. Para o desbloqueio, deve ser apresentada solicitação formal à área de Tecnologia da Informação, para que efetue o desbloqueio. A senha definida expira a cada noventa dias, podendo ser trocada a qualquer momento pelo Colaborador, desde que cumpra os requisitos acima. Eventos de incidente de segurança da informação podem iniciar um processo de expiração de senhas, conforme procedimento específico.

8.8. Todos os sistemas e aplicações instalados na FRAM Capital possuem mecanismo que oculta a visualização das senhas, ao serem digitadas. Os usuários de rede podem ter diferentes acessos, de acordo com as suas atividades. É vedado, de forma a resguardar a segurança da informação da FRAM Capital, a utilização de usuários não nominais por Colaboradores, assim como a utilização do usuário de terceiro.

8.9. Instalações de *softwares* de qualquer natureza devem ser solicitadas à área de Tecnologia da Informação, que verifica eventuais impactos, executando-a ou não, de acordo com o resultado da verificação. O histórico de acessos dos usuários é controlado de forma individualizada.

9. GESTÃO DE ACESSOS

9.1. Os acessos são concedidos pela área de Tecnologia da Informação e autorizados pela área de *Compliance*. As concessões, revisões e exclusões de acesso são mapeadas e respeitam a segregação de atividades da FRAM Capital. Além disso, os acessos são rastreáveis, a fim de garantir que todas a ações passíveis de auditoria possam ser atreladas ao usuário e Colaborador respectivo, responsável pela ação.

9.2. Na contratação de Colaboradores ou na alocação interna de Colaboradores, o gestor é responsável pelo pedido de acesso aos recursos necessários aos seus Colaboradores geridos, de junto às áreas de Tecnologia da Informação e *Compliance*. É de responsabilidade de cada Colaborador a leitura e a compreensão das regras aplicáveis aos recursos aos quais lhe é concedido acesso.

9.3. A revisão de usuários e acessos ativos é feita anualmente, buscando identificar eventuais conflitos de interesses e inconsistências.

9.4. Em caso de identificação de conflitos de interesses em relação aos acessos aprovados pelo gestor, o gestor da área de Tecnologia da Informação encaminhará uma solicitação à área de *Compliance*, para o adequado endereçamento do caso. Os riscos devem ser identificados por meio de um processo estabelecido para a análise de vulnerabilidades, ameaças e impactos sobre os ativos de informação da FRAM Capital. A identificação dos cenários de riscos de segurança da informação é discutida nos Comitês Executivo e de Riscos e *Compliance*.

9.5. Por fim, os testes de identificação de vulnerabilidades e fragilidades na infraestrutura da FRAM Capital são realizados anualmente.

10. PROTEÇÃO DE DADOS PESSOAIS

10.1. A presente Política deve ser lida em conjunto à Política de Privacidade e Proteção de Dados da FRAM Capital, disponível em https://www.framcapital.com.

11. TRATAMENTO E PLANO DE RESPOSTAS A INCIDENTES

11.1. Eventuais incidentes de segurança da informação ou cibernéticos da FRAM Capital devem ser reportados às áreas de Tecnologia da Informação e de Compliance, tão logo sejam identificados por qualquer Colaborador. Qualquer incidente de segurança da informação ou cibernético será discutido pelo Comitê de Riscos e Compliance.

11.2. Caso o incidente envolva o vazamento de dados, o DPO deverá ser imediatamente comunicado e acionado, para o adequado endereçamento da ocorrência.

11.3. A FRAM Capital pode, a seu exclusivo critério, adotar plano de contingências, se necessário, com vistas à manutenção dos serviços prestados.

11.4. Na ocorrência de determinados incidentes de segurança da informação ou cibernética, além da comunicação às áreas internas, a área de *Compliance* avaliará a necessidade e pertinência da comunicação às autoridades competentes, conforme o caso e

nos termos da lei e regulamentação em vigor.

12. PHISHING

12.1. O *phishing* é uma técnica utilizada por cibercriminosos para induzir usuários a erro, por meio de e- mails maliciosos. O e-mail de *phishing* tem como principal objetivo atrair a atenção dos usuários. São modalidades de *phishing*:

a) quando o e-mail é supostamente enviado por um meio de comunicação oficial (autoridades governamentais, instituições financeiras, lojas de comércio eletrônico, sites populares, etc.); e

b) quando o e-mail disponibiliza formulários, para preenchimento, ou *softwares*.

12.2. A FRAM Capital orienta os usuários de seus sistemas a não clicarem em *links* suspeitos e a estarem atentos a erros de português, ofertas, benefícios extraordinários, e mensagens que contenham qualquer forma de conteúdo suspeito, inconsistente ou de origem desconhecida.

12.3. Caso, por motivos diversos, o usuário acesse *link* suspeito, inconsistente ou enviado por remetente desconhecido, deve entrar em contato com as áreas de Tecnologia da Informação e *Compliance* imediatamente, para que estas tomem as ações mitigadoras cabíveis e possam mapear e impedir danos.

13. BACKUP

13.1. Os procedimentos de *backup*, testes e recuperação de dados realizados em caso de crise são executados de forma automática e abrangem os dados gravados nos diretórios de rede de cada equipe e nos servidores de dados e aplicativos. A FRAM Capital conta com *backup* nos servidores de arquivos e *Disaster Recovery*. Todos os serviços e Colaboradores estão com a proteção de *backup* ativos, garantindo a disponibilidade dos dados.

14. TESTES

14.1. É de responsabilidade de todos os Colaboradores observar as regras desta Política, para evitar a facilitação de ações criminosas contra ou relacionadas às informações geridas pela FRAM Capital. De todo modo, foi definido um programa de segurança cibernética com as seguintes etapas:

a) identificação e avaliação de riscos;

b) ações de prevenção e proteção;

c) monitoramento e testes; e

d) vigência.

14.2. A responsabilidade pela implementação, validação e testes cabe à área de Compliance e pode contar com o auxílio externo especializado para melhorar a segurança do ambiente em questão, bem como de analistas de Tecnologia da Informação, para avaliar e identificar potenciais riscos cibernéticos. A partir da identificação dos riscos, são analisados os princípios da confidencialidade, integridade, disponibilidade, confiabilidade, segurança, prevenção e prestação de contas.

14.3. Os referidos testes são conduzidos, no mínimo, anualmente.

15. TREINAMENTO

15.1. Considerando que o nível de segurança depende da cooperação de todos os Colaboradores, é promovido treinamento periódico, com o intuito de orientar todos os Colaboradores em relação:

a) às responsabilidades e os procedimentos relacionados a cada área de atuação;
b) os acessos e regras de uso de forma apropriada; e
c) as suas obrigações.

15.2. Considerando que todos os Colaboradores são devidamente instruídos, em caso de descumprimento de qualquer das regras estabelecidas nesta Política ou de sua suspeita, de acordo com os procedimentos estabelecidos, a FRAM Capital poderá utilizar os registros realizados pelos sistemas de monitoramento eletrônico e telefônico, para apurar a conduta de seus Colaboradores, sendo facultado o acesso a quaisquer informações, contatos, documentos e arquivos gerados pelas atividades profissionais desenvolvidas na FRAM Capital ou que transitem pelos seus Sistemas de Informação.

16. REVISÃO DO DOCUMENTO

16.1. A periodicidade de revisão deste documento é, no mínimo, anual.

17. APROVAÇÃO DO DOCUMENTO

17.1. A presente Política foi aprovada pelo Comitê de Riscos e Compliance.

HISTÓRICO DAS ATUALIZAÇÕES			
DATA	**VERSÃO**	**AUTOR**	**REVISOR**
Fevereiro/2013	1.0	Cesare Rivetti	-
Dezembro/2016	2.0	Roberto Adib	Veridiana Moleta
Julho/2018	3.0	Roberto Adib	Maria Ximena Roche
Abril/2019	4.0	Roberto Adib	Maria Ximena Roche

Dezembro/2019	4.1	Roberto Adib	Maria Ximena Roche
Fevereiro/2020	5.0	Roberto Adib	Maria Ximena Roche
Novembro/2021	6.0	Victor Obara	Laís Codeço
Janeiro/2022	7.0	Bruna Veiga	Victor Obara
Março/2023	8.0	Amanda Fonseca	Laís Codeço
Março/2024	9.0	Amanda Fonseca	Gustavo Tonetti
Agosto/2025	10.0	Roberta Fauth	Fabio Sato