FRAM Capital

Política de Segurança da Informação e Cibernética

Março/2023

Sumário

I. 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.

1.2. Sendo assim, o maior objetivo desta Política é a redução das vulnerabilidades da instituição a ameaças à segurança da informação, assim como a prevenção, detecção e redução da vulnerabilidade a incidentes relacionados com o ambiente cibernético.

1.3. Esta instituição estabelece as diretrizes para compor um programa completo e consistente de segurança da informação e riscos cibernéticos, visando:

a) Proteção do valor e da reputação da empresa;

b) 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 estarão disponíveis a todas as partes autorizadas, quando necessário;

c) Identificação de violações de Segurança Cibernética, estabelecendo ações sistemáticas de detecção, tratamento e prevenção de incidentes, ameaças e vulnerabilidades nos ambientes físicos e lógicos, objetivando a mitigação dos riscos cibernéticos, política de *backup* de informações dentre outros;

d) Garantia da continuidade de seus negócios, protegendo os processos críticos de interrupções inaceitáveis causadas por falhas ou desastres significativos;

e) Conscientizar, educar e treinar os colaboradores por meio de Política Corporativa de Segurança Cibernética, normas e procedimentos internos aplicáveis as suas atividades diárias;

f) Estabelecer e melhorar continuamente um processo de Gestão de Riscos de Segurança Cibernética.

g) Confiabilidade e adequação à legislação de todas as informações sob gestão da área de Tecnologia da Informação (“TI”), definindo procedimentos para mitigar os impactos de eventuais incidentes, prevenindo interrupções e assegurando a proteção de todos os ativos, dados, programas e equipamentos.

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

II. ABRANGÊNCIA E RESPONSABILIDADES

2.1. Esta Política da FRAM Capital (“Fram Capital” ou “Companhia”) se estende ainda a todos os colaboradores acionista/sócios, diretores, associados, funcionários permanentes ou temporários e estagiários (“Colaboradores”), bem como fornecedores e prestadores de serviço da Fram Capital, devendo todos os colaboradores pautar a sua conduta em conformidade com os valores de boa-fé, ética, lealdade e veracidade e, ainda, pelos princípios gerais aqui estabelecidos. Esta política é revisada com suporte da área de TI e é divulgada aos colaboradores, principalmente após suas atualizações.

2.2. A utilização dos recursos de tecnologia da informação será monitorada, com a finalidade de detectar divergências entre as normas que integram a presente Política e os registros de eventos monitorados, fornecendo evidências nos casos de incidentes de segurança.

2.3. A gestão do processo de incidentes de vazamento de informações, como este processo, está sob responsabilidade do *Data Protection Officer* (“DPO”) e é endereçada no Manual de Gestão de Incidentes da instituição.

III. REGULAMENTAÇÃO ASSOCIADA

Esta Política possui base legal e normativa nas leis vigentes, nas melhoras práticas de segurança da informação do mercado e em resoluções de órgãos reguladores, aos quais a Fram Capital é fiscalizada e aderente.

Lei 13.709, de 14 de agosto de 2018
Lei Geral de Proteção de Dados Pessoais (LGPD).

Lei 13.853, de 8 de julho de 2019
Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências.

Resolução BACEN nº 4893, de 26 de fevereiro de 2021
Dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições autorizadas a funcionar pelo Banco Central do Brasil.

Resolução BACEN nº 4.557, de 23 de fevereiro de 2017
Dispõe sobre a estrutura de gerenciamento de riscos, a estrutura de gerenciamento de capital e a política de divulgação de informações.

ISO 27001/2013
Estabelecer, implementar, manter e melhorar continuamente um Sistema de Gestão de Segurança da Informação (SGSI) – Anexo A – Objetivos e Controles.

Guia de Cibersegurança ANBIMA
Programa de Segurança Cibernética da ANBIMA

IV. SEGURANÇA DA INFORMAÇÃO

4.1. Os gestores de cada equipe são responsáveis pela aderência dos membros dos seus times aos princípios e procedimentos necessários. colaboradores que compõem a área de TI, administrando as instalações, são responsáveis pelos procedimentos de segurança dos equipamentos e acessos. Além disso, há aderência formal das pessoas relacionadas com a instituição mediante conhecimento e assinatura do Termo de Confidencialidade de Informações e Proteção de Dados.

4.2. Através da equipe de TI, a Fram Capital efetuará avaliações de risco regulares do ambiente de segurança da informação, para estimar a vulnerabilidade em potencial e garantir que as medidas de segurança reduzem os riscos e suprem patamares apropriados. Os riscos da nossa avaliação interna incluem:

a) Usuários com nível de acesso superior ao necessário;
b) Garantir a segurança de cada terminal e dos materiais impressos em nome da Fram Capital;
c) Uso da internet ou de aplicativos que permitam invasão;
d) Mensagens eletrônicas forjadas – como *Phishing;*
e) Uso de credenciais ou acesso de terceiros.

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

a) Confidencialidade: garantimos que o acesso à informação seja obtido somente por pessoas autorizadas e quando for necessário;
b) Disponibilidade: garantimos que as pessoas autorizadas tenham acesso à informação, sempre que necessário;
c) Integridade: garantimos a exatidão e a completude da informação e dos métodos de seu processamento;

d) Confiabilidade: garantimos a transparência nos tratos com os públicos envolvidos;
e) finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
f) adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
g) necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
h) livre acesso: garantia, aos titulares de dados pessoais, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
i) qualidade dos dados: garantia, aos titulares de dados, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
j) transparência: garantia, aos titulares de dados, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
k) segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
l) prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
m) não discriminação: impossibilidade de realização do tratamento de dados para fins discriminatórios ilícitos ou abusivos;
n) responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

4.4. Esta Política se aplica a todas as informações presentes na Fram Capital, que podem existir de diversas maneiras:

a) Escrita em papel;
b) Armazenada e/ou transmitida por meios eletrônicos;
c) Exibida na mídia;
d) Falada em conversas formais e informais.

4.5. Independente da forma ou o meio pelo qual a informação for apresentada/compartilhada, ela sempre deverá estar protegida adequadamente, de acordo com controles definidos neste documento.

4.6. Todos os usuários que utilizam Sistemas de Informação ("SI") e fazem parte da Organização devem, obrigatoriamente, conhecer e obedecer a esta Política, sendo responsabilidade de cada colaborador o seu cumprimento. Caso algum usuário perceba qualquer incidente de segurança da informação, deve-se informar o ocorrido imediatamente às áreas de *Compliance* e Tecnologia.

4.7. Somente atividades lícitas, éticas e administrativamente admitidas devem ser realizadas pelos usuários na utilização dos SI na Fram Capital.

4.8. As informações de propriedade da Fram Capital devem ser utilizadas apenas para os propósitos devidos. Os usuários não podem, em qualquer hipótese, apropriar-se dessas informações, seja em CDs, *uploads, downloads, pen drives* ou qualquer outra mídia de armazenamento de dados. Todos os documentos produzidos por qualquer SI na Fram Capital são de propriedade exclusiva desta instituição.

4.9. A identificação do usuário (por meio de seu usuário de rede, senha, ou outro meio qualquer) é pessoal e intransferível, qualificando-o como responsável por todas as atividades desenvolvidas utilizando tal identificação.

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

4.11. A Fram Capital, por meio de suas áreas de *Compliance* e Tecnologia da Informação, se reserva o direito de monitorar, automaticamente, o tráfego efetuado através das suas redes de comunicação, incluindo o acesso à Internet o uso do correio eletrônico e a obediência às normas/procedimentos escritos neste documento.

4.12. Todas as informações deverão ter classificação de segurança, para que haja proteção adequada quanto ao seu acesso e uso.

4.13. 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.

4.14. Os acessos a plataformas e equipamentos são disponibilizados pela Fram Capital, enquanto o colaborador integre seu quadro. Não é permitido o compartilhamento a terceiros e o uso que não atenda exclusivamente aos objetivos corporativos.

4.15. 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 sistemas, a ela licenciados, para prevenir, detectar ou minimizar os impactos decorrentes do uso inadequado ou em descumprimento às suas políticas e legislação que lhe for aplicável. Os dados e os equipamentos são propriedade exclusiva da Fram Capital, e desta forma, são passíveis de monitoramento.

4.16. Para assegurar que as informações tratadas estejam adequadamente protegidas, a Fram Capital adota os seguintes processos:

a) Gestão de Ativos da Informação: Entende-se por ativos da informação tudo o que pode criar, processar, armazenar, transmitir e até excluir informação. Podem ser tecnológicos (*software* e *hardware*) e não tecnológicos (pessoas, processos e dependências físicas). Os ativos devem ser identificados de forma individual, inventariados e protegidos de acessos indevidos, fisicamente e logicamente, e ter documentação e planos de manutenção atualizados anualmente. Métodos de proteção e segurança são aplicados aos ativos da informação para proteger acessos indevidos ou não autorizados vindos de meio externo ou internos, como dispositivos móveis (*pendrives*, cartões de memória, HD externo ou equivalentes) ou mídias removíveis (*smartphones*, câmeras, gravadores e equivalentes). Estes dispositivos estão sob atenção especial e restrições para evitar infiltração de fragilidades ou facilitar vazamento de informações. Os equipamentos pertencentes à Fram Capital de uso pessoal/coletivo, servidores de dados e aplicativos, de qualquer porte, estão dotados de mecanismos de proteção contra vírus e *malwares*.

b) Transferência de informações/dados: Estabelece diretrizes e padrões para os procedimentos de transferência de dados internamente e externamente, com proteção e segurança, através de análises e investigação de vulnerabilidades nos recursos de processamento da informação, permitindo correções/adequações tempestivas, minimizando os riscos de violação de dados e mitigando o vazamento dos dados tratados. Os recursos adotados constam de itens técnicos dos contratos com fornecedores.

4.17. As informações devem ser classificadas de acordo com a confidencialidade e as proteções necessárias, nos seguintes níveis:

a) Informação Restrita: é toda informação associada aos interesses estratégicos da Fram Capital, de posse da diretoria, dos comitês e dos gestores das áreas. Seu acesso deve ser limitado a um número reduzido de pessoas autorizadas. Se revelada ou adulterada, pode trazer sérios prejuízos financeiros, favorecer a concorrência e gerar impactos negativos nos negócios e à imagem da instituição ou dos demais agentes do negócio. 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, auditoria e colaboradores previamente designados.

c) Informação Confidencial: é toda informação transmitidas por meios escritos, eletrônicos, verbais ou quaisquer outros e de qualquer natureza, cujo conhecimento está limitado a colaboradores que, pela natureza da função que desempenham, dela necessitam para o exercício profissional. Sua divulgação ou adulteração pode trazer impactos negativos aos negócios e na gestão de processos, ou prejuízos à imagem da instituição ou aos demais agentes do negócio.

d) Informação de Uso Interno: é toda informação cujo conhecimento e uso estão restritos exclusivamente 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.

e) Informação de Uso Público: é toda informação que pode ser divulgada para o público externo à Fram Capital, sem implicações de proteção e controle de acesso. Tais informações somente serão publicadas com permissão da instituição.

4.18. Caso um colaborador tenha acesso a qualquer informação à qual não tenha sido previamente autorizada, este deverá, imediatamente, abster-se de usar tal informação em seu favor, para clientes da Fram Capital ou para terceiro, além de informar a Diretoria acerca do ocorrido.

4.19. A Fram Capital veda expressamente aos colaboradores efetuar qualquer tipo de operação no mercado financeiro baseada em informações privilegiadas, bem como recomendá-las ou sugeri-las a terceiros. Fica ressaltado que a realização de operações no mercado financeiro mediante o emprego de informações privilegiadas fere as regras estabelecidas pelo BACEN e pela CVM, sendo punível cível e criminalmente.

4.20. Todas as Informações Confidenciais recebidas devem ser analisadas pelo colaborador atentamente, principalmente, mas não limitado a:

a) *Insider Trading*: significa a compra e/ou venda de títulos e valores mobiliários através do uso de informação privilegiada, com a intenção de auferir benefício para si ou para terceiros;
b) *Front Running*: significa a realização de operações de compra e/ou venda de títulos e valores mobiliários de forma a concluir e/ou obter vantagem econômica antecipadamente a outros;
c) Qualquer outra prática que não esteja alinhada com os interesses da FRAM Capital e seus clientes.

4.21. Na classificação de um conjunto de informações que apresentam diversos níveis de confidencialidade, deve-se adotar a classificação de maior nível presente no conjunto.

4.22. Para isto, devem ser consideradas as necessidades relacionadas aos negócios, o compartilhamento ou restrição de acesso e os impactos no caso de utilização indevida das informações. Tal classificação será atribuída inicialmente pelo gestor da informação devendo ser obedecida por quem recebê-la.

V. SEGURANÇA CIBERNÉTICA

5.1. A aplicação do programa de segurança cibernética da Fram Capital é norteada pelos seguintes fatores:

a) Identificação/avaliação de riscos (*risk assessment*) – identificação dos riscos internos e externos, dos ativos de hardware, software e processos que precisam de proteção. A mensuração destes riscos é mapeada e evidencia os sistemas críticos da instituição, para protegê-los de forma mais abrangente. São considerados sistemas críticos os sistemas: de bancos vinculados a FRAM Capital; JD Cabine; Britech; Stallos; Sinqia; SELIC; e, E-Guardian.

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, ou seja, buscar impedir previamente a ocorrência de um ataque cibernético, incluindo a programação e implementação de controles. As ações de prevenção já realizadas pela FRAM Capital São: atualização de antivírus, instauração do DLP (para prevenir o desvio/perda de arquivos), a realização de assessment para mensurar possíveis falhas ainda existentes, a execução de sistemas de mapeamento e mitigação de *phishing*, dentre outros.

c) Monitoramento e testes – detecção das ameaças em tempo hábil, de forma a reforçar os controles, caso necessário, e identificar possíveis 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 ocorra quaisquer falhas, perdas ou inconsistências, há ação direta da área de tecnologia da informação e do compliance, se necessário. Já no tocante aos testes de funcionamento dos ambientes de tecnologia e seus desdobramentos, estes são realizados tanto pela área de Auditoria Interna como pela área de Controles Internos.

d) Criação do plano de resposta – ter um plano de resposta, tratamento e recuperação de incidentes, incluindo um plano de comunicação interna e externa, caso necessário. O plano de resposta a incidentes consta disposto, especificamente, no Manual de Gestão de Incidentes. Já o plano de resposta aos demais itens/falhas detectadas, são endereçados com as áreas carentes junto dos departamentos de Auditoria e de Controles Internos.

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

5.2. Conforme sua criticidade, as ações do programa de segurança cibernética divide-se em:

a) Ações críticas: Consiste em correções emergenciais e imediatas para mitigar riscos iminentes;
b) Ações de Sustentação: Iniciativas de curto/médio prazo, para mitigação de risco no ambiente atual, mantendo o ambiente seguro, respeitando o apetite ao risco da Organização e permitindo que ações de longo prazo/estruturantes possam ser realizadas;
c) Ações Estruturantes: Iniciativas de médio/longo prazo que tratam a causa raiz dos riscos e que preparam a Fram Capital para o futuro.

5.3. 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 são controladas por biometria.

5.4. Todos os dispositivos e todo o tráfego de informação estão gerenciados e monitorados de forma centralizada pela área de Tecnologia da Informação e auditado pelo time de suporte. Os dispositivos estão no domínio da Fram Capital.

VI. SEGURANÇA FÍSICA DO AMBIENTE

6.1. A segurança física do ambiente refere-se as medidas de segurança adotadas no ambiente físico da organização, onde contém, ou pretende-se disponibilizar acessos, a ativos de informações sensíveis. Visa a proteção de ativos sensíveis (dados e informações) contra acesso não autorizado, modificação ou destruição, assim como, a proteção do próprio sistema de tecnologia da informação contra uso não autorizado ou danos físicos.

6.2. O processo de segurança física estabelece controles relacionados à concessão de acesso físico ao ambiente somente a pessoas autorizadas, de acordo com a criticidade das informações previamente mapeadas e declaradas.

6.3. Uma das formas de proteção das instalações e das áreas seguras é realizada por meio do estabelecimento de perímetros de segurança física. Possui uma entrada restrita para pessoas autorizadas, sendo necessário baixar um aplicativo ou reconhecimento facial. Em caso de visitantes, o controle de acesso é realizado na recepção e antes de subir, ligam para a recepcionista autorizar.

VII. NORMAS DE UTILIZAÇÃO

✓ Da Internet

7.1. O acesso à Internet na Fram Capital é uma concessão feita aos usuários, e não um direito. Disto decorre que se deve utilizá-la prioritariamente para atividades ligadas ao trabalho, quando em horário comercial.

7.2. Os usuários devem utilizar a Internet de forma adequada e diligente, em conformidade com a lei, a moral e a ordem pública, abstendo-se de objetivos ou meio para a prática de atos ilícitos, lesivos aos direitos e interesses da Organização ou que, de qualquer forma, possam danificar, inutilizar, sobrecarregar ou deteriorar os recursos tecnológicos e documentos de qualquer tipo.

7.3. É proibida a divulgação e/ou compartilhamento indevido de informações sigilosas em listas de discussão, bate-papo ou *softwares* de mensagens eletrônicas.

7.4. Usuários com acesso à Internet não podem efetuar *upload* de qualquer *software* cuja licença pertence à Organização, o mesmo ocorrendo para dados de propriedade da Fram Capital. Exceção feita a casos especiais, mediante autorização do(s) responsável(is) pelo(s) *software*(s) e/ou dado(s).

7.5. Downloads serão autorizados desde que a fonte seja confiável. Para instalação de *softwares* oriundos da Internet, será necessária autorização da área de *Compliance*.

7.6. Cada usuário é responsável por zelar pelo cumprimento ao estabelecido pela presente norma e por todas as atividades realizadas por intermédio de seu usuário de rede. As contas de serviço têm acesso restrito a determinadas pastas de rede na Fram Capital.

7.7. Não é permitida a utilização de *software peer-to-peer*, acesso a sites de relacionamento (como Facebook, Tweeter, Instagram e afins), pornografia, pedofilia e outros contrários à lei.

✓ De Meios de Comunicação Informais

7.8. 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 comunicação autorizados são monitorados, independentemente de sua ciência e anuência, não sendo reservado qualquer direito sobre o material coletado.

✓ Do Correio Eletrônico

7.9. 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.

7.10. É vedada a qualquer usuário a utilização do correio eletrônico para quaisquer das 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 (seja pela lei, seja pela presente norma), lesivos aos direitos e interesses da Fram Capital, que possam danificar, inutilizar, sobrecarregar ou deteriorar hardware e/ou software, documentos e arquivos de qualquer tipo, ou que contrariem a moral, os bons costumes e a ordem pública;
d) Envio intencional 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 e/ou caderno de endereços para distribuição de mensagens que não tenham relação com o interesse funcional da Fram Capital ou a devida permissão do responsável pelas listas e/ou caderno de endereços em questão;
f) Todo e qualquer uso do correio eletrônico não previsto nesta política que afete a Fram Capital de forma negativa.

7.11. Qualquer violação aos itens dispostos neste capítulo não garante a preservação sigilosa dos dados constantes no correio eletrônico em questão.

✓ De Contas e Senhas para Usuários

7.12. Com o intuito de controlar a distribuição de direitos de acesso a sistemas de informação e serviços, a Fram Capital estabelece estas normas para evitar o uso inapropriado de senhas e, consequentemente, diminuir o risco de falhas e violações de sistemas.

7.13. Todas as senhas de rede são pessoais e intransferíveis, devendo ser mantidas em sigilo. Cada usuário é responsável por sua senha e será responsabilizado pelo mau uso dessa senha.

7.14. Esta instituição efetua o estabelecimento de senhas da seguinte forma:

a) Senha de rede - Os usuários finais deverão estabelecer senhas de acesso ao notebook ou ao desktop de forma a respeitar o seguinte padrão: ter , no mínimo, seis a oito caracteres, sendo obrigatório o uso de letras maiúsculas e minúsculas, números e caracteres especiais (@ % ^; .). Na ocorrência de várias tentativas de ingresso erradas, a senha de acesso à rede da Fram Capital é bloqueada. Para desbloqueio, somente com solicitação formal à área de TI, a qual efetuará o desbloqueio como administrador. O tempo de expiração da

senha é de noventa dias, no máximo, podendo ser trocada a qualquer momento pelo colaborador, desde que cumpra os requisitos acima. Eventos de incidente de segurança da informação poderão iniciar um processo de expiração de senhas, conforme procedimento específico.

b) Senha de sistemas críticos - são considerados sistemas críticos os sistemas de bancos vinculados a FRAM Capital; JD Cabine; Britech; Stallos; Sinqia; SELIC; e, E-Guardian. Os parâmetros mínimos de configuração de senha deverão seguir o mesmo padrão estabelecido para as senhas de rede, com exceção dos usuários de bancos, os quais possuem critérios básicos próprios.

7.15. Todos os sistemas e aplicações instalados na Fram Capital possuem mecanismo que oculta a visualização das senhas para utilização desses sistemas/aplicações.

7.16. Os usuários de rede terão privilégios administrativos que se enquadrem às suas atividades, o mesmo ocorrendo nas permissões aos diretórios de rede e seus conteúdos. É vedado, de forma a resguardar a segurança da informação desta instituição, a utilização de usuários não nominais por colaboradores, assim como a utilização de usuários que não sejam em nome próprio.

7.17. Instalações de softwares de qualquer natureza devem ser solicitadas à área de TI, a qual irá analisar o impacto dessa instalação, executando-a ou não, de acordo com o resultado dessa avaliação.

7.18. O histórico de acessos dos usuários é controlado de forma individualizada, através do recurso que detém a informação. No caso de acessos a dados armazenados em servidores, os eventos de segurança evidenciam os acessos.

VIII. GESTÃO DE ACESSOS

8.1. Os acessos são concedidos pela área de tecnologia e autorizados pela área de Compliance. As concessões, revisões e exclusões de acesso são mapeados e respeitam a segregação da instituição.

8.2. Além disso, os acessos são rastreáveis, a fim de garantir que todas a ações passíveis de auditoria possam identificar individualmente o colaborador responsável pela ação, para sua devida responsabilização.

8.3. Na contratação ou na transferência de área, cada gestor de área é responsável pelo pedido de acesso aos recursos necessários aos seus colaboradores geridos, de modo que as áreas de TI e *Compliance*, juntamente, estejam cientes e concordem com a habilitação adequada. É de responsabilidade de cada colaborador a leitura e a compreensão dos funcionamentos dos recursos aos quais tem acesso. A revisão de acessos atuais é feita anualmente, buscando sanar conflitos de interesse e manter a matriz de acessos atualizada.

8.4. Em caso de identificação de conflitos dos acessos aprovados pelo gestor, em relação à matriz de segregação de funções, o gestor de TI encaminhará uma solicitação à área de *Compliance*, para avaliação da concessão.

8.5. Os riscos devem ser identificados por meio de um processo estabelecido para análise de vulnerabilidades, ameaças e impactos sobre os ativos de informação da Fram Capital, para que sejam recomendadas as proteções adequadas.

8.6. A identificação dos cenários de riscos de segurança da informação é discutida nos Comitês Executivo e de Riscos e *Compliance*.

8.7. Os testes de identificação de vulnerabilidades e fragilidades na infraestrutura interna e externa da Fram Capital são realizados anualmente e são avaliados pela alta direção tendo seus planos de ação considerados e adotados conforme deliberação desses comitês.

IX. LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD)

9.1. A Lei Geral de Proteção de Dados Pessoais (LGPD) de 14 de agosto de 2018, regula todo tratamento de dados pessoais na FRAM Capital, e visa a promoção de uma proteção igualitária dos dados pessoais de todos os cidadãos.
9.2. A disciplina da proteção de dados pessoais tem como fundamentos:
a) o respeito à privacidade;
b) a autodeterminação informativa;
c) a liberdade de expressão, de informação, de comunicação e de opinião;
d) a inviolabilidade da intimidade, da honra e da imagem;
e) o desenvolvimento econômico e tecnológico e a inovação;
f) a livre iniciativa, a livre concorrência e a defesa do consumidor; e
g) os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.
9.3. A legislação se fundamenta em diversos valores e tem como principais objetivos:

a) Assegurar o direito à privacidade e à proteção de dados pessoais dos usuários, por meio de práticas transparentes e seguras, garantindo direitos fundamentais.
b) Estabelecer regras claras sobre o tratamento de dados pessoais.
c) Fortalecer a segurança das relações jurídicas e a confiança do titular no tratamento de dados pessoais, garantindo a livre iniciativa, a livre concorrência e a defesa das relações comerciais e de consumo.
d) Promover a concorrência e a livre atividade econômica, inclusive com portabilidade de dados.

9.4. Os dados confidenciais podem ser classificados de acordo com a sua natureza, são eles:
a) Dados pessoais - qualquer informação que possa tornar uma pessoa física identificada ou identificável;
b) Dados sensíveis - Qualquer dado pessoal que diga respeito a origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, bem como dado referente à saúde ou à vida sexual, dado genético ou biométrico.
9.5. O consentimento é definido na LGPD como uma "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada".
9.6. Assim, esse tipo de autorização poderá ser **livre** (o titular não pode ser obrigado a dar o seu consentimento e este também não pode ser obtido de forma automática, como em caixas de textos já pré-selecionadas ou em casos em que a própria navegação na plataforma já pressupõe o aceite de todas as condições); **informada** (o titular deve compreender exatamente o que ele está consentindo, por que e para que antes de tomar qualquer decisão. Além disso, a informação deve ser passada de forma completa, transparente e simples); e, **inequívoca** (não pode haver dúvidas sobre a verdadeira aceitação daquelas condições pelo titular e as empresas devem se esforçar ao máximo para garantir essa compreensão).
9.7. O consentimento necessita ser documentado de forma a demonstrar a manifestação de vontade do titular. A autorização deverá ter finalidades determinadas e textos genéricos, enganosos, abusivos ou que não tenham sido apresentados com transparência em momento anterior serão considerados nulos.
9.8. O consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado. Qualquer tipo de mudança de finalidades, condições ou compartilhamento dos dados pessoais, a FRAM Capital informará de forma destacada, tendo o titular o direito de voltar atrás caso discorde das alterações.
9.9. O término do tratamento de dados pessoais ocorrerá nas seguintes hipóteses:

a) verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada;
b) fim do período de tratamento;
c) comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento conforme disposto no § 5º do art. 8º da Lei de LGPD, resguardado o interesse público; ou
d) determinação da autoridade nacional, quando houver violação ao disposto nesta Lei.

9.10. A FRAM Capital nomeou como DPO o Sr. Roberto Adib, e os contatos se dão através do e-mail LGPD@framcapital.com. O e-mail mencionado acima é divulgado no diretório interno e no site institucional.

9.11. O DPO possui como objetivo a mitigação de problemas relativos à captação e tratamento de dados da FRAM Capital, assim como evitar multas de compliance digital e outras penalidades por descumprimento da LGPD.

9.12. Dessa forma, o DPO constituído possui como responsabilidade:
a) O aconselhamento e verificação dos processos das áreas responsáveis pelo tratamento de dados;
b) Garantia da conformidade da empresa com a LGPD;
c) Aceitação das reclamações e comunicações dos titulares dos dados que a empresa está captando e tratando;
d) Prestação de esclarecimentos e solucionar problemas relativos aos dados;
e) Cooperar com a ANPD (Autoridade Nacional de Proteção de Dados), estabelecendo contato, quando necessário;
f) Orientação dos funcionários sobre o respeito às práticas de proteção de dados pessoais, assim como alinhamento com a área de compliance acerca do conteúdo do treinamento;
g) Execução das demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

X. TRATAMENTO E PLANO DE RESPOSTAS A INCIDENTES

10.1. Os incidentes de segurança da informação e cibernéticos da Fram Capital devem ser reportados às áreas de Tecnologia da Informação e de Compliance. O processo de tratamento destes incidentes resta mapeado em documento exclusivo denominado Manual de Gestão de Incidentes, o qual está sob posse as áreas envolvidas. Para casos de incidentes de vazamento de informações o DPO deverá ser imediatamente comunicado e acionado para realizar a gestão deste processo.

10.2. A Fram Capital possui procedimentos existentes em caso de incidentes de eventos, tomando as ações e os prazos de forma razoável e apropriada ao caso concreto, identificando a vulnerabilidade e os riscos em questão. Ademais, há salvarguardas reativas contra ocorrências de quaisquer intrusões, para reparar e reportar ameaças caso haja um incidente.

10.3. A Fram Capital possui em vigor o Manual de Gestão de Incidentes, o qual formaliza as medidas essenciais que necessitam ser adotadas em caso da existência de um. Esta instituição também poderá ativar o seu plano de contingência, se necessário,de forma a efetuar a manutenção dos serviços prestados.

10.4. Em caso de incidente, além da comunicação às áreas internas, a área de compliance prosseguirá com a comunicação ao Banco Central do Brasil que se fizer necessária.

XI. *PHISHING*

11.1. O *phishing* é uma técnica utilizada por cibercriminosos para driblar os usuários, através de envio de e-mails maliciosos, a fim de obter informações pessoais como senhas, cartão de crédito, CPF, número de contas bancárias, entre outros.

11.2. O e-mail de *phishing* possui o objetivo de atração da atenção dos usuários, seja pela possibilidade de obter alguma vantagem financeira, seja por curiosidade ou seja por caridade.

11.3. Modalidades de *Phishing*:

a) Quando tentam se passar pela comunicação oficial de instituições conhecidas como: Bancos, Lojas de comércio eletrônico, entre outros sites populares;
b) Quando tentam induzir os usuários a preencher formulários com os seus dados pessoais e/ou financeiros, ou até mesmo a instalação de softwares maliciosos que possuem o objetivo de coletar informações sensíveis dos usuários;

c) Esta instituição recomenda aos usuários de seus sistemas (diretores, sócios, colaboradores etc.) que não clique em links suspeitos (por exemplo com erros de português, ofertas e benefícios extraordinários) através de computadores e dispositivos móveis relacionados a FRAM Capital; que não exponha dados pessoais em redes sociais.

11.4. Caso, por motivos diversos, o usuário clique na comunicação fraudada, é obrigatório entrar em contato com as áreas de tecnologia e compliance para que estes tomem as ações mitigadoras cabíveis, e estes possam mapear/impedir maiores danos, caso tenha havido vazamento de credenciais.

XII. BACKUP

12.1. Este capítulo estabelece diretrizes e padrões para 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 privativos de cada equipe e nos servidores de dados e aplicativos.

12.2. 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, conforme a regulação aplicável exige. Todos os procedimentos de backup estão mais detalhados em manual específico.

XIII. TESTE DE STRESS

13.1. É de responsabilidade de todos os colaboradores observar as regras desta Política, para evitar a facilitação de possível ação criminosa a partir das 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;
d) Vigência.

13.2. A responsabilidade pela implementação, validação e testes caberá à área de Compliance e poderá contar com o auxílio externo especializado para melhorar a segurança do ambiente em questão, bem como de analistas de tecnologia para avaliar e identificar potenciais riscos da estrutura empregada. A partir da identificação dos riscos, serão analisados os princípios da confidencialidade, integridade e disponibilidade.

XIV. TREINAMENTO

14.1. Considerando que o nível de segurança depende da cooperação de todos os colaboradores, é promovido treinamento anual, com o intuito de orientar sobre:

a) As responsabilidades e os procedimentos relacionados a cada área de atuação;
b) Acessos e limites de uso de forma apropriada; e
c) Os requerimentos e obrigações de confidencialidade.

14.2. A Fram Capital se empenha para aderência aos requerimentos regulatórios e as diretrizes desta Política, de modo que orienta seus colaboradores sobre a estrutura e os procedimentos de gerenciamento.

14.3. Considerando que todos os colaboradores são devidamente instruídos e auxiliados, sempre que houver a ocorrência de descumprimento ou suspeita ou indício de descumprimento de quaisquer das regras estabelecidas nas Normas Internas e, ou, nas regulações aplicáveis às atividades da Fram Capital, de acordo com os procedimentos estabelecidos, o Compliance poderá se utilizar dos registros e sistemas de monitoramento eletrônico e telefônico disponíveis para verificar a conduta dos colaboradores envolvidos, sendo facultado o acesso a quaisquer informações, contatos, documentos e arquivos gerados pelas atividades profissionais desenvolvidas na Fram Capital, ou que transitem pela sua infraestrutura de TI. Eventualmente, medidas internas podem ser tomadas em caso de necessidade.

14.4. Realizamos ações de disseminação de questões sobre segurança da informação e cibernética por meio treinamentos e e-mail corporativo.

XV. ESTRUTURA DE GOVERNANÇA

15.1. A Diretoria Executiva é o órgão máximo de deliberação da Fram Capital. Sua atuação é pautada pelo comprometimento da instituição com as melhores práticas na governança e no processo de Segurança da Informação, melhorando continuamente esta Política, sua governança, seus processos, seus procedimentos, os controles internos e a cultura organizacional sobre este assunto. Neste 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 toda equipe atuante no processo possa alcançar seus objetivos;
c) Zelar pela prevenção incidentes relacionados à Segurança da Informação; e
d) Avaliar a efetividade desta política e dos procedimentos relacionados à Segurança da Informação.
a) Investimento em recursos necessários ao processo de prevenção de incidentes;
b) Incentivo e prática contínua a disseminação de uma cultura de gestão de riscos;
c) Manutenção de colaboradores experientes, qualificados, motivados, continuamente treinados e comprometidos com suas atribuições e responsabilidades; com os objetivos e metas estabelecidos pela administração e com a prestação de serviços de qualidade; e
d) Incentivo a segregação de funções nas diversas áreas envolvidas no processo de prestação desses serviços.

15.2. São atribuições do Comitê de Riscos e Compliance:

a) Aprovar os manuais de procedimentos que envolvem a Segurança da Informação;
b) Analisar os relatórios de *Compliance* e decidir pela comunicação do(s) cliente(s) enquadrado(s) como sensíveis;
d) Analisar as demandas levadas a pauta das reuniões do Comitê de Risco e *Compliance* emitindo pareceres e decisões de acordo com esta Política e com a legislação aplicável; e
e) Zelar pelos manuais que envolvem a Segurança da Informação, descritos neste documento.

15.3. É de responsabilidade da área de Tecnologia da Informação:

a) A manutenção contínua do ambiente tecnológico seguro e que suporte a operação da companhia;
b) Oferecer suporte técnico e operacional às demais áreas nos assuntos relacionados à Segurança da Informação; e
c) Manter seus processos aderentes às disposições estabelecidas nesta Política.

15.4. É de responsabilidade área de Compliance:

a) Divulgar e dar conhecimento a todos os colaboradores sobre as normas e os procedimentos relativos à Segurança da Informação;
b) Dar manutenção aos controles internos e manuais relativos ao tema;
c) Orientar todos os Colaboradores de acordo com as regras estabelecidas nesta Política;
d) Prover adequado treinamento aos Colaboradores com programação permanente e de amplo alcance; e
e) executar rotinas de diligência sobre a aderência dos processos estabelecidos às diretrizes da presente Política.

15.5. É de responsabilidade área de Controles Internos:

a) Realizar testes, mapear falhas e conduzir planos de ação para correção.

XVI. REVISÃO DO DOCUMENTO

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

XVII. APROVAÇÃO DESTA POLÍTICA

17.1. A presente política foi aprovada pelo Comitê Executivo.

HISTÓRICO DAS ATUALIZAÇÕES			
DATA	**VERSÃO**	**AUTOR**	**REVISOR**
Fev/2013	1.0	Cesare Rivetti	-
Dez/2016	2.0	Roberto Adib	Veridiana Moleta
Jul/2018	3.0	Roberto Adib	Maria Ximena Roche
Abr/2019	4.0	Roberto Adib	Maria Ximena Roche
Dez/2019	4.1	Roberto Adib	Maria Ximena Roche
Fev/2020	5.0	Roberto Adib	Maria Ximena Roche
Nov/2021	6.0	Victor Obara	Laís Codeço
Jan/2022	7.0	Bruna Veiga	Victor Obara
Mar/2023	8.0	Amanda Fonseca	Laís Codeço