POLÍTICA DE SEGURANÇA CIBERNÉTICA - HUB FINTECH

CONTROLE DE ALTERAÇÕES

Revisão	Data	Local da Revisão	Descrição
0	12/05/2021	-	Emissão inicial
1	25/07/2022	Toda a Política	Revisão Geral da Política; Alteração do *e-mail* da Gerência de Segurança da Informação para **<si@fintechmagalu.com.br>**.
2	27/09/2023	Toda a Política	Revisão Geral da Política, com alteração nos itens 2, 3, 4, 5.5, 5.14, 6.3, 6.4 e 7
3	27/12/2023	Itens 3 e 4.3	Alteração nos itens 3 e 4.3
4	27/08/2024	Toda a Política	Ajuste nos itens 2, 3, 4.2, 4.6, 5.2 e 5.9

LISTA DE DISTRIBUIÇÃO

Função
Todos os administradores, colaboradores, prestadores de serviços e parceiros da Hub Fintech.

LISTA DE TREINAMENTO

Áreas funcionais
Todos os administradores, colaboradores, prestadores de serviços e parceiros da Hub Fintech.

Elaborado/Revisado por:
Gerência de Segurança da Informação
Gerência de Infraestrutura
Diretoria de *Compliance*, Integridade e PLD
Departamento Jurídico

Aprovado por:

Aprovado por:
Diretoria Colegiada, em 29/08/2024.

1. OBJETIVO

Garantir a proteção e a manutenção da integridade, disponibilidade, confidencialidade e privacidade dos dados e de todas as informações sob responsabilidade da Hub Fintech, e dos sistemas de informação utilizados, inclusive da computação em nuvem, além de contribuir para instituição de diretrizes que viabilizem a prevenção, detecção e redução de vulnerabilidades a incidentes relacionados com o ambiente cibernético.

2. TERMOS E DEFINIÇÕES

- **Ativos Tecnológicos:** No contexto de Segurança da Informação, é qualquer bem ou direito que tenha valor para a Instituição, como computadores, dispositivos móveis, sistemas, aplicativos, bases de dados, informações, sala de servidores, entre outros.
- **Colaboradores:** São todos que têm ou tiveram algum vínculo com a Instituição, assim compreendido: empregados, ex-empregados, aprendizes, ex-aprendizes, estagiários, ex-estagiários, prestadores de serviço, ex-prestadores de serviços, diretores, sócios, terceiros, parceiros ou ex-parceiros, visitantes que têm, terão ou tiveram acesso às informações da Instituição e/ou utilizam, utilizarão ou utilizaram sua infraestrutura tecnológica, mesmo após o término do regime jurídico a que estavam submetidos.
- **Confidencialidade:** Garantir que as informações tratadas sejam de conhecimento exclusivo de pessoas especificamente autorizadas.
- **Comitê de crise de Tecnologia:** Composto por ao menos um representante de cada uma das seguintes áreas: Segurança da Informação, Tecnologia da Informação e Privacidade de Dados.
- **Comitê de Privacidade:** O comitê é composto pelo Encarregado pelo tratamento de dados pessoais ("Encarregado" ou "Encarregado de Dados"), representantes da Diretoria de *Compliance*, Integridade e PLD, da Diretoria de Tecnologia, e, um diretor designado da própria estrutura da Instituição . Os representantes deverão ser designados pelo Diretor ou Head da área. O Comitê é responsável pelas definições relacionadas ao direcionamento do Programa de Privacidade de Dados e a avaliação de projetos de alta criticidade para a Instituição.

- **Comitê Executivo de Gestão da Fintech (Controladora - COMITÊ):** em observância ao seu regimento próprio, tem por finalidade acompanhar a gestão administrativa e financeira da Hub Fintech, avaliando as estratégias relacionadas ao negócio da área, deliberando acerca das necessidades financeiras e/ou operacionais para atingi-las; e, aprovando-as, quando cabível, em conformidade com as alçadas instituídas nesta Política de Alçadas.

- **Comitê Executivo (COMEX):** Comitê com a atribuição de deliberar sobre contratações de alto valor, reorganização orçamentária e outros temas relacionados à gestão da Hub. Composto pelos Diretores, Diretores Estatutários e pelo Diretor Presidente, sendo obrigatória a presença de no mínimo de 2 (dois) diretores estatutários, o Diretor Financeiro e o Diretor da área funcional demandante (ou representante designado) do tema submetido à aprovação. Este Comitê será secretariado pela Diretoria de Compliance, Integridade e PLD.
- ***Cracks***: pequenos *softwares* usados para quebrar um sistema de segurança qualquer. Seu uso mais comum é para transformar programas em versões limitadas, seja em funcionalidade ou tempo de uso, os chamados *sharewares*, em um programa completo, removendo ou enganando o sistema de segurança que limita o uso ou verifica o número serial.
- **Dado:** Para os fins desta Política, dado é o registro do atributo de um ente, objeto ou fenômeno onde registro significa a gravação ou a impressão de caracteres ou símbolos que tenham um significado em algum documento ou suporte físico.
- **Dado em nuvem:** Dado armazenado em servidores de alta disponibilidade via internet.
- **Dado em repouso:** Dado armazenado em computador, servidor, drive externo, dispositivo móvel, e outros que não o movimente de um local para outro.
- **Dado Produtivo:** Dados utilizados no ambiente de produção.
- **Dados Pessoais**: quaisquer informações relativas a uma pessoa natural (“Titular" ou Titular dos Dados”), que possibilite sua identificação individualizada; em especial por referência a um identificador único; como por exemplo, nome, número de identificação ou documento oficial, dados de localização, identificadores eletrônicos, ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, econômica, cultural ou social do titular, ou ainda a combinação de mais de um destes dados.
- **Dados Pessoais Sensíveis**: informações sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou

político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculados a uma pessoa natural.

- **Disponibilidade:** Garantir que as informações estejam disponíveis a todas as pessoas autorizadas a tratá- las.
- **Duplo fator de autenticação:** É um recurso que acrescenta uma camada adicional de segurança para o processo de login da conta, exigindo que o usuário forneça duas formas de autenticação.
- **Falhas de Segurança:** São vulnerabilidades que podem gerar indisponibilidade ou comprometer a segurança dos sistemas.
- **Hub Fintech:** Significa a Hub Instituição de Pagamento S.A., suas subsidiárias integrais e empresas controladas, direta ou indiretamente, e empresas coligadas.
- **Fornecedores Críticos**: Um fornecedor é considerado crítico nas situações em que o descumprimento de um determinado critério relacionado à contratação pode impactar significativamente o negócio ou as atividades da Instituição.
- **Incidentes Relevantes:** São incidentes capazes de causar risco ou dano relevante para o negócio (exemplos: dados financeiros, contábeis, gerenciais) e, aqueles que possam causar danos materiais ou morais aos titulares.
- **Integridade:** Garantir que as informações sejam mantidas íntegras, sem modificações indevidas – acidentais ou propositais.
- **Privacidade e Proteção de Dados:** Responsabilidade nas atividades de tratamento de Dados Pessoais, seguindo os preceitos estabelecidos pela Lei Geral de Proteção de Dados (Lei nº 13.709/18), tais como finalidade, necessidade, transparência, segurança e não discriminação.
- **Segurança Cibernética:** Todo e qualquer Dado gerado, obtido, adquirido sob responsabilidade da Hub Fintech, é considerado de sua propriedade, devendo ser utilizado exclusivamente para seus interesses.
- **Segurança da Informação:** Preservação da confidencialidade, integridade e disponibilidade de dados e informações. Adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade, também poderão estar envolvidas.
- **Sistema da Informação:** Um conjunto organizado de elementos, podendo ser pessoas, dados, atividades ou recursos materiais em geral. Estes elementos interagem entre si para processar informação e divulgá-la de forma adequada em função dos objetivos de uma

organização.

- **Vazamento de Dados Pessoais**: consiste na violação dos dados pessoais e/ou dados pessoais sensíveis que são indevidamente acessados, coletados e divulgados na internet, por meio da invasão de sistemas de uma organização, por terceiros não autorizados.

3. ATRIBUIÇÕES E RESPONSABILIDADES

Áreas funcionais:	Responsável por:
Diretoria Colegiada	• Avaliar e aprovar a Política de Segurança Cibernética, conforme norma vigente; • Assegurar que a Política de Segurança Cibernética e os objetivos de segurança cibernética estão estabelecidos e são compatíveis com a direção estratégica da organização; • Garantir que os recursos necessários para o sistema de gestão da segurança cibernética estão disponíveis; • Promover a cultura de segurança cibernética e da conformidade com os requisitos do sistema de gestão da segurança cibernética; • Autorizar as exceções da presente política.
Gerência de Segurança de Informação e Segurança Cibernética	• Viabilizar e operacionalizar todos os mecanismos e/ou instrumentos necessários a aplicabilidade desta política; • Garantir que todos os recursos necessários à aplicação da presente política sejam disponibilizados; • Analisar a documentação e os controles implementados validando a aderência dos controles da política. • Propor a implementação de novos controles a fim de aderência regulatória e aumento de maturidade de segurança da informação. • Checar a eficácia e efetividade dos mecanismos instituídos/implantados, pela Instituição, para garantir a segurança cibernética; • Monitorar periodicamente a efetividade da aplicação da presente política, por meio de reporte das áreas operacionais e,

Áreas funcionais:	Responsável por:
	ainda, quando possível, pela execução de Avaliações de Controles de Segurança da Informação; • Desenvolver, implantar e/ou aprimorar as soluções de tecnologia, relacionadas à Segurança da Informação; • Orientar o controle do antivírus/antimalware em todos os servidores, estações de trabalho e *notebooks*; • Garantir a Salvaguarda da licença de uso do antivírus; • Monitorar constante as eventuais vulnerabilidades técnicas dos ativos de informação; • Aplicar testes de intrusão periódicos (*pentest*); • Aplicar controles e procedimentos para correção das vulnerabilidades identificadas, incluindo a proteção contra a instalação de *softwares* maliciosos; • Implantar controles visando a prevenção a vazamento de dados; • Estabelecer conexões de acesso remoto rastreáveis por meio de trilhas de auditoria; • Implantar controles para garantir que as informações sejam conhecidas, alteradas e acessadas somente por pessoas autorizadas, de acordo com a Política de Classificação das Informações; • Avaliar, em conjunto com a Diretoria de Compliance, Integridade e PLD, os riscos inerentes a segurança cibernética nos ativos de tecnologia da informação da Hub Fintech e reportá-los à Diretoria de Tecnologia; • Apoiar a Área de Tecnologia da Informação nas ações que garantam a continuidade de negócios.
Departamento Jurídico	• Monitorar e notificar as áreas interessadas quanto a existência, criação e atualização de legislações vigentes e aplicáveis a Instituição, referentes aos temas de Privacidade, Segurança da Informação, e Segurança Cibernética; • Garantir que terceirizados e fornecedores que manipulam dados originados na Hub Fintech assinem os termos de

Áreas funcionais:	Responsável por:
	confidencialidade e/ou contrato contendo cláusulas de privacidade, segurança da informação e segurança cibernética, de acordo com a prestação de serviços e atividade, se aplicável.
Diretoria de Tecnologia - Segurança Cibernética	• Definir diretrizes relacionadas à segurança cibernética; • Instituir planos de ação e definir respostas a possíveis incidentes de segurança, conforme a Política de Resposta de Incidentes de Segurança da Informação; • Instituir, sempre que necessário e/ou demandado pela Diretoria Colegiada, instrumentos de controle de violações às diretrizes aqui estabelecidas; • Treinar, com o apoio da área de gestão de pessoas, todos os colaboradores, e conscientizá-los acerca das diretrizes e regulamentos de Segurança Cibernética e Segurança da Informação; • Reportar à Diretoria Colegiada qualquer tipo de incidente e/ou violações relacionadas à presente política, assim como os planos de recuperação após incidente cibernético; • Notificar, tempestivamente, à Gerência de PLD/FT e Regulatório, as ocorrências de incidentes relevantes e interrupções dos serviços relevantes, que configurem situação de crise pela Instituição, bem como das providências para o reinício das suas atividades, que devem ser comunicados ao BACEN; • Compartilhar, tempestivamente, com as instituições de pagamento e demais instituições autorizadas a funcionar pelo Banco Central, os incidentes relevantes; • Implantar mecanismo ou instrumento para viabilizar o compartilhamento de informações sobre incidentes relevantes com as instituições de pagamento e demais instituições autorizadas a funcionar pelo Banco Central; • Informar, à Gerência de PLD/FT e Regulatório, a relação de fornecedores relevantes contratados, que deverão ser comunicados ao BACEN, em até 5 dias da data da contratação;

Áreas funcionais:	Responsável por:
	• Propor e, quando necessário, conduzir a execução de ações corretivas ou preventivas pertinentes a qualquer matéria relacionada à segurança cibernética; • Definir e nomear os responsáveis pelas informações tratadas; • Nomear os responsáveis por cada um dos sistemas de informação; • Notificar, tempestivamente, a Gerência de Privacidade e Proteção de Dados, as ocorrências de incidentes de segurança da informação que envolvam dados pessoais; • Informar, ao Comitê de Privacidade, nos casos de incidentes que envolvam dados pessoais, quais dados pessoais foram afetados, os titulares envolvidos e as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo; • Assegurar a governança dos dados, a fim de garantir a confidencialidade, disponibilidade e integridade das informações; • Aplicar o princípio do privilégio mínimo de acesso a todas solicitações, condicionando a concessão de acesso à necessidade efetiva e, ainda, considerando anonimização de dados sensíveis; • Treinar o responsável pelos dados e informações.
Gerência de Infraestrutura	• Gerenciar, descrever e testar, com apoio da Área de Segurança da Informação, os planos de continuidade de negócios; • Realizar cópias de segurança (*backup restore),* garantindo a recuperação de dados essenciais à infraestrutura de tecnologia; • Garantir a segregação e segmentação de ambiente de rede, para reduzir os riscos de acessos ou modificações acidentais e/ou não autorizadas; • Executar o controle do antivírus/antimalware em todos os servidores, estações de trabalho e *notebooks*; • Assegurar o suporte e manutenção da VPN; • Garantir a proteção do ambiente de todos os ativos críticos de tecnologia da informação;

Áreas funcionais:	Responsável por:
	• Implantar mecanismos de controle de acesso, a fim de garantir a confidencialidade dos dados durante a sua transmissão e armazenamento; • Revisar periodicamente as autorizações concedidas; • Aplicar técnicas de criptografia para a proteção da confidencialidade e da integridade das informações críticas, armazenadas ou trafegadas pelos ativos de informação, conforme a Política de Criptografia; • Garantir a utilização de senhas segura, obedecendo aos requisitos de segurança e complexidade, além do duplo fator de autenticação obrigatório nos acessos às contas dos usuários; • Monitorar os *E-mails* dos colaboradores e serviços *Google*.
Diretoria de *Compliance*, Integridade e PLD	• Apoiar a Diretoria de Tecnologia na elaboração de políticas e procedimentos e na adoção e institucionalização de mecanismos e/ou instrumentos de controle relacionados aos requisitos estabelecidos na presente política; • Auxiliar a Diretoria de Tecnologia na divulgação e nos treinamentos acerca dos requisitos de segurança Cibernética e Segurança da informação; • Ajudar na elaboração e implantação de planos de ação corretivos e preventivos; • Sugerir adequações das políticas, controles e procedimentos; • Conduzir processos de verificação de Compliance, com a finalidade de checar a eficácia e efetividade dos requisitos estabelecidos na presente política; • Avaliar, em conjunto com a Gerência de Segurança da Informação e Segurança Cibernética, os riscos inerentes à segurança cibernética nos ativos de tecnologia da informação da Hub Fintech e reportá-los à Diretoria de Tecnologia.
Comitê de Crise de Tecnologia	• Avaliar o incidente que ocasionou a interrupção de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem contratados;

Áreas funcionais:	Responsável por:
	• Propor solução(ões) para a crise; • Envolver todas as partes necessárias e determinar as atribuições de cada uma; • Decidir sobre o curso de ação.
Comitê de Privacidade	• Tratar os incidentes de segurança da informação que resultarem em violação de Dados Pessoais e/ou Dados Pessoais Sensíveis; • Recomendar a adoção de medidas remediadoras para mitigar os riscos reputacionais, financeiros e/ou de sanções à Instituição; • Propor melhorias aos mecanismos ou instrumentos de controle e monitoramento às diretrizes estabelecidas no Manual do Programa de Privacidade de Dados Pessoais; • Comunicar à Diretoria Colegiada da Instituição os incidentes de privacidade que representem risco alto e possam causar impactos negativos relacionados à reputação da organização e gerar externalidades financeiras e/ou que possuam o condão de gerar aplicação de sanções relevantes.
Gerência PLD/FT e Regulatório	• Comunicar, tempestivamente, ao Bacen as ocorrências de incidentes relevantes e interrupções dos serviços relevantes, que configurem situação de crise pela Instituição, bem como das providências para o reinício das suas atividades; • Comunicar ao Bacen as contratações de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem, em até 10 dias úteis da contratação.
Auditoria Corporativa	• Auditar os processos, procedimentos e mecanismos de segurança Cibernética e Segurança da informação, apontando, quando identificado/necessário, não conformidades e oportunidades de melhorias; • Auditar, periodicamente, ou sempre que houver necessidade, os ativos tecnológicos e da informação e sua utilização.

Áreas funcionais:	Responsável por:
Gestão de Pessoas	• Informar as diretrizes presentes nesta política aos novos colaboradores, • Apoiar a Diretoria de Tecnologia no treinamento de todos os colaboradores e na conscientização acerca das diretrizes e regulamentos de Segurança Cibernética e Segurança da Informação; • Assegurar que todos os ativos fornecidos aos colaboradores, durante a vigência de seu contrato, sejam devolvidos no momento em que ocorrer a extinção do vínculo; • Informar às áreas responsáveis acerca da remoção de acessos físicos ou acessos lógicos aos sistemas de informação no momento em que ocorrer o desligamento do colaborador ou o encerramento do contrato de prestação de serviço e as alterações de cargo/área.
Gerências e demais lideranças	• Fazer e garantir que seus liderados façam todos os treinamentos necessários, com o intuito de assegurar que as medidas de segurança da informação referentes à sua área estão sendo observadas; • Avaliar, periodicamente, os privilégios atribuídos a cada Perfil de Acesso.
Colaboradores	• Respeitar as diretrizes de Segurança Cibernética e Segurança da Informação estabelecidas nas políticas; • Fazer todos os treinamentos indicados para o exercício de sua função, e, sempre que sentir necessidade, procurar ajuda/esclarecimentos com a área de Segurança da Informação; • Conhecer e cumprir os procedimentos de segurança, homologado pela Gerência de Segurança da Informação, com o objetivo de proteger as informações da Hub Fintech; • Notificar a àrea de Segurança da Informação, sempre que identificar uma violação das diretrizes citadas nesta política; • Notificar a àrea de Segurança da Informação caso identifique a existência de fragilidades ou eventos de falha na Segurança Cibernética e Segurança da Informação;

Áreas funcionais:	Responsável por:
	• Sugerir melhorias de controles, políticas e procedimentos, quando identificar necessidade; • Assinar, no momento da contratação, o Termo de Aceite ao Código de Compromisso de Confidencialidade e Sigilo.

4. DIRETRIZES PARA SEGURANÇA CIBERNÉTICA

Todo e qualquer dado e informação gerado, obtido, adquirido ou sob responsabilidade da Hub Fintech é considerado de sua propriedade, devendo ser utilizado exclusivamente para seus interesses.

O dado consiste em informação e, consequentemente, um ativo de extremo valor e importância, tratando-se de um elemento fundamental para a estratégia de negócio da Instituição.

O uso, tratamento, disponibilização e/ou compartilhamento de dados da Instituição, por todos os colaboradores, parceiros, terceiros, administradores e acionistas deverão respeitar os requisitos definidos nesta Política e nas demais políticas, procedimentos e manuais relacionados.

Em linhas gerais, os dados e as informações da Instituição não devem ser divulgados, mesmo que internamente, para pessoas não autorizadas. A divulgação em ambiente externo exige prévia autorização da Instituição, sendo controlada com identificação do armazenamento, inclusive sítio de armazenamento, ficando disponível, em caso de questionamento, pelo Banco Central.

Com a finalidade de assegurar a observância dessas diretrizes, são adotadas medidas de segurança que previnem o compartilhamento indevido de dados pessoais e de dados sensíveis da Instituição, e o uso inadequado da infraestrutura da Instituição.

A Hub Fintech trabalha para que todos os seus colaboradores, parceiros e terceiros, administradores respeitem e assegurem a confidencialidade, integridade e disponibilidade de dados e/ou informações a que tiverem acesso e/ou fizerem uso.

Em razão da constante evolução tecnológica, é obrigação do colaborador adotar todo e qualquer procedimento de segurança, homologado pela área de segurança da informação, que esteja ao seu alcance, visando proteger todas as informações da Hub Fintech, ainda que não esteja previsto nesta Política.

4.1 Diretrizes de Dados e Dados em Nuvem

- O acesso aos dados e informações deverá ser restrito e controlado. Neste sentido, deverão ser implantados controles para garantir que os dados e informações sob responsabilidade da Instituição sejam conhecidos, alterados e acessados somente por pessoas autorizadas.
- Os colaboradores da Hub Fintech devem assinar, no momento da contratação, o Termo de Aceite ao Código de Compromisso de Confidencialidade e Sigilo, e renová-lo anualmente;
- Os ativos relacionados com a geração, armazenamento e processamento de informações deverão ser controlados e inventariados;
- A utilização dos ativos deverá ser previamente autorizada, e seu uso restrito às atribuições necessárias para que os colaboradores exerçam suas atividades profissionais;
- O responsável pela informação deve implantar todos os controles necessários para a devida proteção da informação, de acordo com a respectiva classificação; e
- A geração, armazenamento e processamento de dados em nuvem deverão ser autorizados, controlados e inventariados pela Instituição.

4.2 Contratação de Serviços de Processamento e Armazenamento de Dados e de Computação em Nuvem

Previamente à contratação de serviços de processamento e armazenamento de dados e de computação em nuvem, a Hub Fintech deve verificar, registrar e evidenciar quanto à capacidade do potencial prestador de serviços de assegurar:

- Acesso da Instituição às informações a serem processadas ou armazenadas pelo prestador de serviço;
- A confidencialidade, a integridade, a disponibilidade e a recuperação dos dados e das informações processadas ou armazenadas pelo prestador de serviço;

- A sua aderência a certificações exigidas pela Instituição para a prestação do serviço a ser contratado;
- A sua aderência às legislações brasileiras aplicáveis, como a Lei Geral de Proteção de Dados (Lei 13.709/18);
- O acesso da Instituição aos relatórios elaborados por empresa de auditoria especializada independente, contratada pelo prestador de serviço, relativos aos procedimentos e aos controles utilizados na prestação dos serviços a serem contratados;
- O provimento de informações e de recursos de gestão adequados ao monitoramento dos serviços a serem prestados;
- A identificação e a segregação dos dados dos usuários finais da Hub Fintech, por meio de controles físicos ou lógicos; e
- A qualidade dos controles de acesso voltados à proteção dos dados e das informações dos usuários finais da Instituição.

Importante: A avaliação da relevância do serviço a ser contratado, deve ser feito pela área responsável pela contratação com apoio da área de Segurança da Informação da Hub Fintech, devendo considerar a criticidade do serviço e a sensibilidade dos dados e das informações a serem processados, armazenados e gerenciados pelo contratado, levando em conta, inclusive, a classificação da informação.

Para os fins da regulamentação em vigor, a avaliação para contratação de prestador de serviços de computação em nuvem, abrange a disponibilidade à Hub Fintech (Instituição de pagamento contratante), sob demanda e de maneira virtual, de ao menos um dos seguintes serviços:

I - processamento de dados, armazenamento de dados, infraestrutura de redes e outros recursos computacionais que permitam à instituição contratante implantar ou executar softwares, que podem incluir sistemas operacionais e aplicativos desenvolvidos pela instituição ou por ela adquiridos;

II - implantação ou execução de aplicativos desenvolvidos pela instituição contratante, ou por ela adquiridos, utilizando recursos computacionais do prestador de serviços; ou

III - execução, por meio da internet, de aplicativos implantados ou desenvolvidos pelo prestador de serviço, com a utilização de recursos computacionais do próprio prestador de serviços.

A Hub Fintech deverá adotar medidas a fim de garantir, que no âmbito da prestação dos serviços contratados, sejam cumpridos todos os requisitos definidos na legislação e regulamentação vigente e, ainda, a confiabilidade, a integridade, a disponibilidade, a segurança e o sigilo das informações tratadas.

Toda vez que a Instituição contratar novos serviços relevantes de processamento, armazenamento de dados e de computação em nuvem, a Gerência do Regulatório e PLD deverá comunicar, em até dez dias, a contratação dos serviços ao Banco Central do Brasil, conforme orientações da Área de Segurança da Informação.

Tal comunicação deve conter as seguintes informações:

I - a denominação da empresa contratada;

II - os serviços relevantes contratados; e

III - a indicação dos países e das regiões em cada país onde os serviços poderão ser prestados e os dados poderão ser armazenados, processados e gerenciados. Assim, a Instituição deve definir, previamente à contratação, os países e as regiões em cada país onde os serviços poderão ser prestados e os dados poderão ser armazenados, processados e gerenciados, no caso de contratação no exterior.

Nota: As alterações contratuais que impliquem na modificação dos serviços pactuados, também devem ser comunicadas ao Banco Central do Brasil, em até dez dias após a alteração contratual.

A contratação de novos serviços relevantes de processamento, armazenamento de dados e de computação em nuvem prestados no exterior deve observar os requisitos da legislação e resolução em vigor.

Os contratos para prestação de serviços relevantes de processamento, armazenamento de dados e computação em nuvem devem conter cláusulas dispondo sobre:

I - a indicação dos países e da região em cada país onde os serviços poderão ser prestados e os dados poderão ser armazenados, processados e gerenciados;

II - a adoção de medidas de segurança para a transmissão e armazenamento dos dados citados no inciso anterior;

III - a manutenção, enquanto o contrato estiver vigente, da segregação dos dados e dos controles de acesso para proteção das informações dos usuários finais;

IV - a obrigatoriedade, em caso de extinção do contrato, de:

a) transferência dos dados citados no inciso I, deste parágrafo, ao novo prestador de serviços ou à instituição de pagamento contratante; e

b) exclusão dos dados citados no inciso I, pela empresa contratada substituída, após a transferência dos dados prevista na alínea "a" e a confirmação da integridade e da disponibilidade dos dados recebidos.

V - a privacidade e proteção de dados pessoais, se a relação contratual envolver tratamento de informações pessoais.

Importante: Todos os Contratos de Prestação de Serviço da Hub Fintech deverão conter os requisitos previstos na legislação vigente e ser validados pelo Departamento Jurídico.

4.3 Diretriz de Gerenciamento de Segurança

O gerenciamento dos controles de segurança deve viabilizar que os procedimentos operacionais sejam desenvolvidos, implantados e mantidos ou modificados de acordo com os objetivos estabelecidos nesta Política, assegurando a eficácia e a efetividade do Programa de Segurança da Informação da Instituição.

Importante: Nos casos de incidentes classificados como relevantes, de acordo com a metodologia definida no Item 4.5, a Hub Fintech deve adotar iniciativas para compartilhamento de informações sobre incidentes relevantes, ao Banco Central, às outras instituições de pagamento e às demais instituições autorizadas a funcionar pelo Banco Central do Brasil.

4.4 Diretrizes para Cultura de Segurança Cibernética

A Hub Fintech deve fomentar a cultura de segurança cibernética em todos os níveis da instituição, para isso, deve:

- Divulgar todas as políticas, procedimentos e manuais relacionados a segurança cibernética e segurança da informação aos colaboradores e fornecedores relevantes;
- Divulgar o *"ANEXO I - RECOMENDAÇÕES E INSTRUÇÕES DE SEGURANÇA CIBERNÉTICA PARA CLIENTES E USUÁRIOS",* desta Política em sítio eletrônico (*website*) para que todos tenham acesso (clientes, prestadores de serviços e outros);

- Treinar, no mínimo, anualmente, todos os seus colaboradores para conhecerem quais são os requisitos necessários de garantia da segurança cibernética ou, também, sempre que a política é atualizada;
- Realizar campanhas periódicas de Segurança Cibernética, a fim de enfatizar e manter a importância e conscientização sobre o tema, além do aculturamento quanto ao tratamento e segurança dos Dados;
- Reportar, periodicamente, à Diretoria Colegiada a evolução da implantação, acompanhamento e resultados dos treinamentos de segurança cibernética.

4.5 Diretrizes em caso de violações de dados e incidentes cibernéticos e avaliação da relevância do incidente

- É responsabilidade de todo colaborador informar à Gerência de Segurança da Informação qualquer ação que possa violar a confidencialidade, integridade e disponibilidade dos dados e informações da Instituição, por meio do *e-mail* **<si@fintechmagalu.com.br>**, conforme Procedimento de Resposta a Incidentes - Hub Fintech.
- Toda suspeita de violação de dados ou confirmação de incidente de segurança deve ser investigado e avaliado, pela Gerência de Segurança da Informação, tais como: (i) acesso não autorizado, acidental ou ilícito, que resulte na destruição, perda, alteração, vazamento; ou (ii) qualquer forma de tratamento de dados inadequada ou ilícita, os quais possam ocasionar riscos, sejam eles:

    a) Risco aos direitos e liberdades do titular ou proprietário dos dados;
    b) Risco à imagem / reputação da Instituição;
    c) Risco Financeiro; e
    d) Outros tipos de riscos, impróprios ao negócio.

Importante: quando a suspeita de violação ou confirmação do incidente envolver dados pessoais, a Gerência de Privacidade de Dados deve ser acionada.

- Os resultados identificados devem ser reportados à Diretoria Colegiada, com os detalhe dos impactos, incluindo informações sobre o tipo de incidente; data e hora; ações adotadas contendo, no mínimo, a rotina, os procedimentos, os controles e as tecnologias utilizadas na prevenção e na resposta ao incidente; área responsável por implantar ou implementar as ações; descrição do vazamento de dados, quando houver, e relevância dos dados e do incidente. Esse detalhamento fará parte do relatório anual conforme disposto no item 4.5.1.

- Na hipótese da materialização do incidente de segurança da informação resultar em violação de Dados Pessoais e/ou Dados Pessoais Sensíveis*, a área de Segurança da Informação deverá atuar em conjunto com o Comitê de Privacidade, em cumprimento às determinações da Lei Geral de Proteção de Dados Pessoais ("LGPD"), relacionadas a Incidentes de Segurança;
- Sob suspeita de qualquer violação, a Área de Segurança da Informação poderá retirar o equipamento em posse dos colaboradores, sem aviso prévio, para realizar a investigação;

***Importante:** O DPO deverá ser imediatamente notificado e deverá ser envolvido em todo o processo de tratativa do incidente.

4.5.1 Relatório anual sobre implementação do plano de ação e de resposta a incidentes cibernéticos

O plano de ação e de resposta a incidentes cibernéticos deve visar à implementação da Política de Segurança Cibernética, abrangendo:

I) as ações a serem desenvolvidas para adequar as estruturas organizacionais e operacionais aos princípios e às diretrizes da presente política;

II) as rotinas, os procedimentos, os controles e as tecnologias a serem utilizados na prevenção e na resposta a incidentes, em conformidade com as diretrizes desta política ; e

III) a área responsável pelo registro e controle dos efeitos de incidentes relevantes.

O Relatório anual sobre a implementação do plano de ação e de resposta a incidentes deverá ser elaborado com a data base de 31 de dezembro e abordar, no mínimo, os seguintes pontos:

a) a efetividade da implantação das ações relacionadas à adequação da estrutura organizacional e operacional da Instituição aos princípios e diretrizes desta Política;

b) o resumo dos resultados obtidos na implantação das rotinas, dos procedimentos, dos controles e das tecnologias utilizados na prevenção e na resposta a incidentes;

c) os incidentes relevantes ocorridos, relacionados com o ambiente cibernético, contendo, no mínimo, as seguintes informações: tipo de incidente, data e hora, ações remediadoras, área responsável pela tratativa, áreas afetadas e avaliação de impacto, e, ainda, as rotinas, procedimentos, controles e tecnologias utilizados na prevenção e na resposta de novos

incidente, área responsável pelo registro e controle dos efeitos de incidentes relevantes, descrição se houve vazamento de dados e relevância dos dados e do incidente.

d) os resultados dos testes de continuidade dos serviços de pagamento prestados, considerando cenários de indisponibilidade ocasionada por incidentes; e

e) previsão de período para verificação de eficácia do plano de ação implementado.

Em conformidade com a regulamentação em vigor, o Relatório deve ser apresentado à Diretoria Colegiada, até 31 de março do ano seguinte ao da data-base.

4.6 Diretrizes de Gestão de Riscos de Segurança Cibernética

- É responsabilidade da área de Segurança da Informação, com apoio da área de Gestão de Riscos, avaliar riscos inerentes a segurança cibernética nos ativos de tecnologia da informação da Instituição e reportá-los à Diretoria de Tecnologia e, posteriormente, à Diretoria Colegiada;
- Todo desenvolvimento, aquisição, implantação e grandes mudanças de sistemas que envolvam processamento de dados e informações da Instituição devem ter uma avaliação formal de riscos da área de Segurança da Informação, assim como o direcionamento de requisitos pela Diretoria Colegiada antes de utilizar dados produtivos e sensíveis, inclusive dados pessoais.
- O tratamento e a gestão dos riscos identificados deve ser realizado pela área responsável da Diretoria de Tecnologia, que reportará à Diretoria Colegiada sobre o andamento das ações.

5. PROCEDIMENTOS E CONTROLES ADOTADOS PARA REDUZIR A VULNERABILIDADE A INCIDENTES

5.1 Proteção do ambiente

A Hub Fintech processa as informações, visando garantir a segurança na infraestrutura tecnológica por meio de gerenciamento efetivo (i) do monitoramento, (ii) do tratamento e (iii) da resposta aos incidentes, com o intuito de minimizar o risco de falhas e administrar de forma segura as redes de comunicação.

5.2 Autenticação

O acesso às informações e aos ambientes tecnológicos da Hub Fintech deve ser permitido apenas às pessoas autorizadas pela Instituição - proprietária da informação-, levando em consideração o princípio do menor privilégio, a segregação de funções e a classificação da informação. O controle de acesso aos sistemas é efetuado pela área de Segurança da Informação, e deve contemplar os seguintes controles:

- Utilização de identificadores (credencial de acesso) individualizados, monitorados e passíveis de bloqueios e restrições (automatizados e manuais);
- Utilização do duplo fator de autenticação obrigatório nos acessos às contas dos usuários;
- Remoção de autorizações dadas a usuários afastados ou desligados ou que tenham mudado de função; e
- Revisão periódica das autorizações concedidas.

5.3 Gestão de Incidentes de Segurança Cibernética - *Cyber* Ataque

Possíveis ataques à Instituição são identificados por meio de controles de detecção implantados no ambiente, como: filtro de conteúdo, ferramenta de detecção de comportamentos maliciosos, antivírus, antispam, *firewall* de aplicação, entre outros.

5.4 Prevenção a Vazamento de Dados

A Hub Fintech utiliza controle para prevenção de perda de dados, a fim de garantir que dados confidenciais não sejam perdidos, roubados, mal utilizados ou vazados na *web* por usuários não autorizados.

5.5 Testes periódicos de segurança dos sistemas de informações, em especial dos mantidos em meio eletrônico

Testes de intrusão internos e externos nas camadas de rede e aplicação devem ser realizados, no mínimo, anualmente, e registrados em relatório anual. O objetivo é validar a segurança nos sistemas computacionais da Hub Fintech, por meio de ataque simulado (***pentest***), que visa identificar pontos de fraqueza na infraestrutura de defesa dos sistemas. O *pentest* possibilita

certificar que as tecnologias de proteção dos recursos digitais não apresentem vulnerabilidades, conforme Procedimento para *Pentest* - Hub Fintech.

5.6 Varredura de Vulnerabilidades

As varreduras das redes internas e externas devem ser executadas periodicamente. As vulnerabilidades identificadas devem ser tratadas e priorizadas de acordo com seu nível de criticidade, além de reportadas para a Diretoria Colegiada (item 4.6), conforme Procedimento de Gestão de Vulnerabilidades - Hub Fintech.

5.7 Controle contas Software Malicioso (*cracks*)

Todos os ativos tecnológicos (computadores, servidores, etc.), que estejam conectados à rede corporativa ou façam uso de dados / informações da Instituição, devem, sempre que possível, ser protegidos com uma ferramenta anti-*malware* determinada pela área de Segurança da Informação.

A ferramenta deve fornecer uma visualização clara das posturas de segurança, ameaças globais e painéis de visualização, com informações importantes sobre detecção, contenção e exclusão de ameaças, para uma correta administração do ambiente de TI.

5.8 Criptografia

Toda solução de criptografia utilizada na Instituição deve seguir as regras de segurança da informação e segurança cibernética estabelecidas pelos órgãos reguladores.

5.9 Senha Segura

Para atender às melhores práticas de segurança e de auditoria, e reduzir o risco de ataques que exploram vulnerabilidades em senhas cadastradas sem critérios de segurança, as senhas devem ser configuradas por meio de solução de gerenciamento de usuários com base centralizada, que exige que todos os usuários do domínio cadastrem senhas, obedecendo aos requisitos de segurança e complexidade: comprimento mínimo de 8 (oito) caracteres, inclusão de número, um símbolo, letras maiúsculas e minúsculas, tempo máximo de duração da senha de 60 dias, limite de 3 (três) tentativas para bloqueio da conta.

5.10 Rastreabilidade

Trilhas de auditoria automatizadas devem ser implantadas em todos os componentes de sistema da Instituição para reconstruir os seguintes eventos:

- Autenticação de usuários (tentativas válidas e inválidas);
- Acesso a informações;
- Ações executadas pelos usuários, incluindo criação ou remoção de objetos do sistema.

5.11 Segmentação da Rede

A Instituição deve possuir segmentação de rede, conforme diretrizes a seguir:

- Computadores conectados à rede corporativa por meio de VPN, não acessíveis diretamente pela Internet;
- Não é permitida a conexão direta de redes de terceiros. Exige-se protocolos de controle remoto aos servidores conectados diretamente na rede corporativa;
- A solicitação de criação, alteração e exclusão de regras nos *firewalls* e ativos de rede são analisados e avaliados pela área de Segurança da Informação antes da execução pela área de Tecnologia da Informação.

5.12 Desenvolvimento Seguro

A Hub Fintech deve manter um conjunto de princípios para desenvolver sistemas de forma segura, para garantir que a segurança cibernética seja projetada e implementada no ciclo de vida de desenvolvimento de sistemas, conforme Procedimento para Desenvolvimento Seguro.

5.13 Cópias de Segurança (*Backup e Restore*)

Um processo de *backup* bem estruturado e implementado de forma correta é essencial para gerenciar a proteção dos dados, prevenir contra ameaças de *ransomware* e estar em conformidade com as legislações de segurança. Por mais robusto e seguro que seja o ambiente e infraestrutura de TI, incidentes podem ocorrer. Por esse motivo, possuir *backups* íntegros e atualizados é muito importante para minimizar uma situação crítica. Assim, com a finalidade de mitigar possíveis impactos indesejáveis, a Instituição realiza os seguintes procedimentos:

- Tipo: *full*, incremental e diferencial;

- Periodicidade: diário e mensal;
- Retenção: mensal, semestral e anual;
- Tipo de armazenamento: *Cloud(s).*

5.14 Serviço de Correio / *E-mail*, Google

Todos os colaboradores devem possuir e-mail corporativo, a ser criado pela Instituição no momento de sua admissão. Neste sentido, a Hub Fintech utiliza plataforma de correio eletrônico e colaboração do fornecedor *Google*, o qual oferece, de forma nativa, diversos recursos de segurança, pois atendem às certificações internacionais de segurança. A solução é disponibilizada na nuvem "*Google Drive*", sendo acessível de qualquer lugar que possua uma conexão com a internet.

A plataforma possui o ATP (*Advanced Threat Protection*) que faz a filtragem dos *e-mails* e auxilia na proteção contra *malware* e vírus desconhecidos, entre outros recursos de segurança embarcados na solução.

5.15 Contingência

Todas as instalações e *sites* da Instituição devem possuir contingenciamento de energia por meio de *no-breaks*, garantindo seu funcionamento em caso de interrupção elétrica.

A infraestrutura deve possuir contingência em zonas distintas, garantindo, assim, a disponibilidade dos sistemas utilizados pela Instituição.

5.16 Planos de Continuidade de Negócios

Os planos de continuidade de negócio objetivam garantir a continuidade dos serviços prestados e deverão ser revisados e atualizados periodicamente, considerando a estrutura organizacional, o porte e a complexidade das operações da Instituição.

5.17 Classificação dos Dados e das Informações

O acesso às informações classificadas como confidencial, restrita, uso interno e público para a Instituição, deverá ser controlado, nos termos da Política de Classificação da Informação. Neste sentido, deverão ser implantados controles para garantir que as informações sejam conhecidas, alteradas e acessadas somente por pessoas autorizadas.

Todos devem tratar as informações de acordo com seu nível de classificação, de forma a protegê-las contra atos ou acessos indevidos ou divulgação não autorizada, mantendo sua confidencialidade, integridade, disponibilidade, autenticidade e conformidade.

O Responsável pela Informação deve implantar todos os controles necessários para a devida proteção da informação, de acordo com a classificação da informação.

Toda informação disponibilizada que não esteja expressamente classificada, deverá ser considerada como "**Uso Interno**", e caso sejam identificadas informações como Dados Pessoais e Dados Pessoais Sensíveis, nos termos da Lei Federal nº 13.709/2018, que dispõe sobre a proteção de dados pessoais, são classificadas automaticamente como "**Confidencial**".

6. DISPOSIÇÕES GERAIS

6.1 Aplicabilidade

Esta Política se aplica a todos os administradores e colaboradores da Instituição de Pagamentos.

6.2 Vigência e aprovação

Esta Política tem vigência a partir da data de sua aprovação e divulgação, podendo ser revisada sempre que necessário.

6.3 Política de Consequências e Violações

Qualquer violação à presente política será passível de penalização, que poderá ser desde advertência verbal até demissão por justa causa e, no caso de ocorrência de danos, reparação do eventual dano causado.

As medidas de consequências adotadas pela Instituição, seja no âmbito interno ou por meio de adoção de medida judicial cabível, serão aplicadas após a avaliação da gravidade do caso concreto e dos impactos causados pela violação.

Compete à Diretoria de *Compliance*, Integridade e PLD apurar os casos relatados e, nos casos mais graves, submeter ao Comitê Disciplinar da Instituição, que deverá, em casos mais críticos, ratificar a sua decisão no COMITÊ.

6.4 Exceções

Todas as exceções às diretrizes das políticas que envolvam a segurança da informação devem ser analisadas e aprovadas pelo COMEX.

Nota 1: O conjunto de diretrizes acima não se esgotam nesta Política e nos regulamentos específicos. Em razão da constante evolução tecnológica, é obrigação do colaborador adotar todo e qualquer outro procedimento de segurança, homologado pela equipe de segurança da informação, que esteja ao seu alcance, visando proteger todas as informações da Hub Fintech, inclusive aquelas relacionadas a dados pessoais, em conformidade com a LGPD.

7. REFERÊNCIA

- Resolução BCB nº 85/2021;
- Código de Ética e Conduta;
- Manual do Programa de Privacidade;
- Política de Aquisição, Desenvolvimento e Manutenção de Sistemas;
- Política de Classificação da Informação;
- Política de Gestão de Privacidade de Dados Pessoais;
- Política de Segurança da Informação;
- Procedimento de Revisão de Acesso;
- Procedimento para Pentest;
- Procedimento de Resposta a Incidentes;
- Procedimento de Gestão de Vulnerabilidades;
- Procedimento de Antimalware e Antivírus;
- NBR ISO/IEC 27001:2013, Sistemas de Gestão de Segurança da Informação;
- NBR ISO/IEC 27002:2013, Código de prática para a gestão da Segurança da Informação;
- Lei Federal nº. 9.279/1996, que regula direitos e obrigações relativos à propriedade intelectual;

- Lei Federal nº 9.609/1998, que dispõe sobre a proteção da propriedade intelectual de programa de computador;
- Lei Federal nº 9610/1998, que altera, atualiza e consolida a legislação sobre direitos autorais;
- Lei nº 12.853, de 14 de agosto de 2013 - Altera os arts. 5º , 68, 97, 98, 99 e 100, acrescenta os arts. 98-A, 98-B, 98-C, 99-A, 99-B, 100-A, 100-B e 109-A e revoga o art. 94 da Lei nº 9.610, de 19 de fevereiro de 1998, para dispor sobre a gestão coletiva de direitos autorais, e dá outras providências;
- Lei Federal nº 12.965/2014, que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil;
- Lei Federal nº 13.709/2018, dispõe sobre a proteção de dados pessoais;
- Resolução nº 4.557, de 23 de fevereiro de 2017 - Banco Central do Brasil;
- Lei nº 13.853, de 08 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;
- Resolução CMN nº 4926, de 24/06/2021 - Altera a Resolução nº 4.557, de 23 de fevereiro de 2017, que dispõe sobre a estrutura de gerenciamento de riscos, a estrutura de gerenciamento de capital e a política de divulgação de informações;
- Medida Provisória nº 1.068, de 6 de setembro de 2021 - Altera a Lei nº 12.965, de 23 de abril de 2014, e a Lei nº 9.610, de 19 de fevereiro de 1998, para dispor sobre o uso de redes sociais.
- Anexo I - Cartilha recomendações e instruções de Segurança Cibernética para clientes e usuários.

8. ANEXOS

ANEXO I - CARTILHA DE RECOMENDAÇÕES E INSTRUÇÕES DE SEGURANÇA CIBERNÉTICA PARA CLIENTES E USUÁRIOS

1. Administração segura de sua senha

O cliente é responsável pelos atos executados com seu identificador (*login / token*), que é único e acompanhado de senha exclusiva para identificação/autenticação individual no acesso à informação e aos recursos de tecnologia. Recomendamos que:

- Mantenha a confidencialidade: memorize e não registre a senha em nenhum lugar. Não divulgue a ninguém, pois compartilhar sua senha é como assinar um cheque em branco;
- Não escreva a senha em local público ou de fácil acesso como, por exemplo, em sua agenda, em um pedaço de papel pregado no seu monitor ou guardado na sua gaveta;

- Troque a senha regularmente ou sempre que existir qualquer suspeita do comprometimento dela;
- Elabore senhas de qualidade, de modo que sejam complexas e de difícil adivinhação. Não utilize números fáceis de serem descobertos, tais como o número da carteira de identidade, do CPF e de outros documentos ou datas de qualquer espécie, como sua senha bancária;
- Não permita o uso do seu equipamento por outras pessoas, enquanto este estiver conectado/ "logado" com a sua identificação;
- Bloqueie sempre o equipamento ao se ausentar;
- Sempre que possível, habilite um segundo fator de autenticação, como por exemplo: SMS e token.

2. Antivírus

Recomendamos que o Cliente e Usuário mantenham uma solução de antivírus atualizada e instalada no computador utilizado, para acesso aos serviços oferecidos pela Hub Fintech.

Adicionalmente, deverão manter o sistema operacional atualizado com as últimas atualizações realizadas.

3. Engenharia Social

Consiste na obtenção de informações importantes por meio de uma conversa informal, aproveitando-se da ingenuidade das pessoas, explorando sua confiança ou a vontade de ajudar. Geralmente o golpista se faz passar por outra pessoa, ou finge ser um profissional de determinada empresa ou área. O indivíduo mal intencionado usa o telefone, *e-mail*, salas de bate-papo, sites de relacionamento e o contato pessoal para conseguir as informações que procura. Por isso:

- Desconfie de abordagens de pessoas que ligam e se identificam como técnicos ou funcionários de determinada firma, solicitando dados sobre sua empresa, sobre o ambiente, sobre você, etc.;
- Evite fazer cadastros pela internet, especialmente fornecendo seus dados pessoais. Se necessário, somente o faça se confiar no site;
- Nunca forneça informações sensíveis, pessoais ou da instituição, por telefone ou outros meios, quando a iniciativa do contato não seja sua;
- Nunca forneça sua senha por telefone, *e-mails* ou outros meios que não sejam o acesso normal aos aplicativos utilizados, ao site do seu banco ou às máquinas de auto-atendimento;

- O lixo pode ser uma fonte de informações para pessoas mal intencionadas. Destrua os documentos que contenham informações sensíveis, pessoais ou corporativas antes de descartá-los no lixo;
- Seja cuidadoso com as informações que você disponibiliza em blogs e redes sociais. Elas podem ser usadas por malfeitores para confirmar os seus dados cadastrais, descobrir dicas e responder perguntas de segurança

3.1. *Phishing*

Trata-se de uma técnica utilizada por cibercriminosos para enganar os usuários, através de envio de *e-mails* maliciosos, para obtenção de informações pessoais como senhas, números de cartão de crédito, número de CPF, número de contas bancárias, entre outros. As abordagens dos *e-mail*s de *phishing* podem ocorrer das seguintes maneiras:

- Quando procuram atrair a atenção dos usuários, seja pela possibilidade de obter alguma vantagem financeira, seja por curiosidade ou seja por caridade;
- Quando tentam se passar pela comunicação oficial de instituições conhecidas como: bancos, lojas de comércio eletrônico, entre outros sites populares;
- 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.

3.2. SPAM

Consistem em *e-mails* não solicitados, que geralmente são enviados para muitas pessoas, possuindo tipicamente conteúdo com fins publicitários. Além disso, os Spams estão diretamente associados a ataques de segurança, sendo eles um dos principais responsáveis pela propagação de códigos maliciosos, venda ilegal de produtos e disseminação de golpes.

3.3. Falso Contato Telefônico

São técnicas utilizadas pelos fraudadores para conseguir informações como dados pessoais, senhas, token, código de identificação do aparelho celular (IMEI) ou qualquer outro tipo de informação para a prática da fraude.

4. Utilização de Aplicativos Hub Fintech em Celular

- Não utilize aparelhos de outras pessoas para acessar aos serviços da Instituição, pois seus dados podem ficar armazenados na memória do celular;
- Funcionalidades de conectividade sem fio, como bluetooth, podem tornar seu aparelho mais vulnerável e suscetível a ataques, envio de vírus e arquivos maliciosos. Recomenda-se manter tais funcionalidades desabilitadas;

- Exclua ou bloqueie o celular da lista de permissão de cadastro de computadores utilizados, caso você troque de número ou de aparelho;
- Desconfie de mensagens solicitando recadastramento de dispositivos, atualização cadastral, ou solicitando informações pessoais, pois pode se tratar de uma tentativa de fraude.

5. Relate qualquer irregularidade à Hub Fintech

- Verifique sempre seu saldo e extrato para certificar-se de que não contenham transações suspeitas ou desconhecidas, caso em que você deve contatar a Hub Fintech e solicitar esclarecimentos;
- Para contato com a Hub Fintech, utilize os números de telefone encontrados no verso do seu cartão;
- Não utilize números de telefones encontrados em sites suspeitos na Internet ou recebidos por *e-mail*, pois pode ser outra fraude; e,
- Fique atento às pessoas ao seu redor e nunca aceite ajuda de desconhecidos.