POLÍTICA DE SEGURANÇA CIBERNÉTICA

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

Lista de Distribuição

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

Lista de Treinamento

Função
Todos os administradores e colaboradores da Hub Fintech.

Elaborado/Revisado por:

Diretoria de Tecnologia

Diretoria de Compliance, Integridade e PLD

Departamento Jurídico

Aprovado por:

DocuSigned by:
Claudio Teruhiko Murasaki
B877758A42234C2...

Claudio Teruhiko Murasaki

Diretor de Tecnologia

1/8/2022 | 14:52 BRT

DocuSigned by:
Fabio Itiro Bonifacio Murakami
166E5DF60629430...

Fabio Itiro Bonifácio Murakami

Diretor de Produtos

28/7/2022 | 17:30 BRT

1. OBJETIVO

Garantir a proteção, a manutenção da privacidade, integridade, disponibilidade e confidencialidade 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 Empresa, 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 Hub Fintech, 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 Empresa 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 Hub Fintech . 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 Hub Fintech.
- **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**: Informações que identificam indivíduos como, por exemplo: nº de CPF, nome completo, nº de RG, email, telefone celular, entre outros.
- **Dados Pessoais Sensíveis**: De acordo com a LGPD, são 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 vinculado a uma pessoa natural.”

- **Disponibilidade:** Garantir que as informações estejam disponíveis a todas as pessoas autorizadas a tratá- las.
- **Falhas de Segurança -** São vulnerabilidades que podem gerar indisponibilidade ou comprometer a segurança dos sistemas.
- **Integridade:** Garantir que as informações sejam mantidas íntegras, sem modificações indevidas – acidentais ou propositais.
- **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.

3. ATRIBUIÇÕES E RESPONSABILIDADES

Cargos/Diretoria	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 a 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 Hub Fintech, para garantir a segurança cibernética; • Monitorar periodicamente a efetividade da aplicação da presente política por meio de reporte das áreas operacionais e, ainda, quando possível, pela execução de Avaliações de Controles de Segurança da Informação; • Investigar e avaliar qualquer suspeita de violação de dados ou confirmação de incidente de segurança; • Registrar e controlar os efeitos dos incidentes de segurança; • Avaliar os impactos operacionais decorrentes da aplicação das normas de Segurança Cibernética; • Certificar que todos os controles de Segurança Cibernética foram desenvolvidos, adquiridos e implantados; • Garantir que todos os controles de Segurança da Informação foram devidamente aprovados pela Diretoria de Tecnologia; • Garantir que os ativos tecnológicos possuam proteção contra Códigos Maliciosos, bem como que recebam as atualizações necessárias; • Assegurar que os acessos nos sistemas de informação sejam feitos mediante identificação única, pessoal, intransferível e com segregação de funções; • Realizar o descarte de informações confidenciais por meio de recursos que resultem na descaracterização do seu conteúdo.
Departamento Jurídico	• Monitorar e notificar as áreas interessadas quanto a existência, criação e atualização de legislações vigentes e aplicáveis a Hub Fintech 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 confidencialidade e o aditivo de Privacidade, Segurança da informação e Segurança Cibernética.
Diretoria de Tecnologia	• Ser o responsável por esta Política de Segurança Cibernética e pelo plano de ação e de resposta a incidentes; • 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 Privacidade, Segurança Cibernética e Segurança da Informação; ● Reportar à Diretoria Estatutária qualquer tipo de incidente e/ou violações relacionadas a presente política, assim como os planos de recuperação após incidente cibernético; ● 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; ● 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, baseando a concessão de acesso somente a necessidade efetiva e, ainda, considerando anonimização de dados sensíveis; ● Treinar o responsável pelos dados e informações.
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 ar 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.
Comitê de Crise de Tecnologia	● Avaliar a interrupção de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem contratados; ● 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	● Acompanhar a efetividade e a eficácia dos mecanismos e/ou instrumentos adotados para garantir a aderência aos requisitos estabelecidos na presente Política;

	• Tratar de incidentes de segurança da informação que resultarem em violação de Dados Pessoais e/ou Dados Pessoais Sensíveis; • Tratar incidentes de privacidade que representem riscos reputacionais, financeiros e/ou de sanções à Hub Fintech; • Acionar planos de contingência, quando previstos, para a situação de risco materializada; • Propor melhorias aos mecanismos ou instrumentos de controle e monitoramento às diretrizes estabelecidas no Programa de Privacidade de Dados Pessoais; • Comunicar, a Diretoria Colegiada da HUB Fintech, os incidentes de privacidade que representem risco alto de impactar a reputação, de gerar externalidades financeiras e/ou que possuam o condão de gerar aplicação de sanções relevantes e • Aprovar exceções, desde que em conformidade legal às boas práticas adotadas pela Hub Fintech, a esta política.
Auditoria Corporativa	• Auditar os processos, procedimentos e mecanismos de segurança Cibernética e Segurança da informação, apontando, quando identificado/necessário, não conformidades, oportunidades de melhorias; • Auditar, periodicamente ou sempre que houver necessidade, os ativos tecnológicos e da informação e sua utilização.
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; • 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; • Sugerir melhorias de controles, políticas e procedimentos, quando identificar necessidade.

4. DIRETRIZES PARA SEGURANÇA CIBERNÉTICA

Todo e qualquer dado e informação gerada, obtida, adquirida ou sob responsabilidade da Hub Fintech é considerada de sua propriedade, devendo ser utilizada exclusivamente para seus interesses.

O dado é informação e, consequentemente, um ativo de extremo valor e importância, sendo esse um elemento fundamental para a estratégia de negócio da empresa.

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

Em linhas gerais, os dados e as informações da empresa não devem ser divulgados, mesmo que internamente, para pessoas não autorizadas. A divulgação em ambiente externo exige prévia autorização da Hub Fintech, 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 evitam o compartilhamento indevido de dados pessoais e de dados sensíveis da empresa, bem como o uso inadequado da nossa infraestrutura.

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 equipe de segurança da informação, que esteja ao seu alcance, visando proteger todas as informações da Hub Fintech, ainda que não 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 Hub Fintech 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 e de Compromisso de Confidencialidade e Sigilo, renovado 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 Hub Fintech.

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 verifica e registra evidência quanto à capacidade do potencial prestador de serviços de assegurar:

- Acesso da Hub Fintech 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 processados ou armazenados pelo prestador de serviço;
- A sua aderência a certificações exigidas pela instituição para a prestação do serviço a ser contratado;
- O acesso da Hub Fintech 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 Hub Fintech.

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 deverá comunicar, em até dez dias após a contratação dos serviços ao Banco Central do Brasil. 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 Hub Fintech 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 modificação das informações contratuais relacionadas acima, também devem ser comunicadas ao Banco Central do Brasil 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.

Importante: Todos os Contratos de Prestação de Serviço da Hub Fintech deverão conter os requisitos previstos na legislação vigente e ser validados pela Diretoria Jurídica.

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 Hub Fintech.

4.4 Diretrizes para Cultura de Segurança Cibernética

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

- Divulga esta política aos colaboradores e fornecedores relevantes;
- Divulga 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);
- Treina, 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;
- Realiza 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 para a 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 área de Segurança da Informação qualquer ação que possa violar a confidencialidade, integridade e disponibilidade dos dados e informações da Hub Fintech, por meio do e-mail si@fintechmagalu.com.br.
- Toda suspeita de violação de dados ou confirmação de incidente de segurança deve ser investigado e avaliado, pela Diretoria de Segurança, 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 Hub Fintech;
    c) Risco Financeiro; e
    d) Outros tipos de riscos, impróprios ao negócio.
- Os resultados identificados devem ser reportados à Diretoria Colegiada, com detalhe dos impactos: tipo de incidente, data, hora, ações implementadas - contendo, no mínimo, a rotina, o procedimentos, os controles e as tecnologias a serem utilizados na prevenção e na resposta ao incidente -, área responsável por implantar ou implementar as ações, descrição se houve vazamento de dados e relevância dos dados e do incidente. Deve ser Acrescentado informações recebidas de empresas prestadoras de serviços a terceiros, se for o caso, bem como controles após incidente, considerando as decisões da Diretoria e impactos para as atividades da Hub Fintech. 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 cooperação com o Comitê de Privacidade na execução do Procedimento de Resposta à Incidentes de Privacidade, em cumprimento às determinações da Lei Geral de Proteção de Dados Pessoais (“LGPD”) relacionadas à 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:** Nessas situações o DPO do Grupo Magalu 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 suas estruturas organizacional e operacional 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 data base 31 de dezembro e abordar, no mínimo, os seguintes pontos:

a) a efetividade da implementação das ações relacionadas à adequação da estrutura organizacional eoperacional da Hub Fintech aos princípios e diretrizes desta Política;

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

c) os incidentes relevantes relacionados com o ambiente cibernético ocorridos no período, contendo, no mínimo, as seguintes informações: tipo de incidente, data, hora, ações implementadas com no mínimo a rotina, procedimentos, controles e tecnologias utilizados na prevenção e na resposta ao 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 regulação em vigor, este 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 Hub Fintech 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 Hub Fintech devem ter uma avaliação formal de riscos da área de Segurança da Informação, assim como o direcionamento de requisitos pela Diretoria Executiva antes de utilizar dados produtivos e sensíveis.

- 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 Hub Fintech - 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);

• 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 Hub Fintech são identificados por meio de controles de detecção implementados 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 internos e externos nas camadas de rede e aplicação devem ser realizados, no mínimo, anualmente, e registrados em relatório anual.

A Hub Fintech possui processos e controles internos de atualização e aplicação de *patchs* dos servidores, plataformas operacionais e aplicações, que garantem um processo contínuo de correção de *bugs* dos sistemas e máquinas.

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).

5.7 Controle contas Software Malicioso

Todos os ativos tecnológicos (computadores, servidores, etc.), que estejam conectados à rede corporativa ou façam uso de dados / informações da Hub Fintech, 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 Hub Fintech 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 oito caracteres, inclusão de número, um símbolo, letras maiúsculas e minúsculas, tempo máximo de duração da senha de 60 dias, limite de 5(cinco) tentativas para bloqueio da conta.

5.10 Rastreabilidade

Trilhas de auditoria automatizadas devem ser implantadas em todos os componentes de sistema 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 Hub Fintech possui segmentação de rede, conforme diretrizes a seguir:

- Computadores conectados à rede corporativa não são 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 por Tecnologia da Informação.

5.12 Desenvolvimento Seguro

A Hub Fintech mantém um conjunto de princípios para desenvolver sistemas de forma segura, garantindo 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, a fim de mitigar possíveis impactos indesejáveis a Hub Fintech 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

A Hub Fintech utiliza plataforma de correio eletrônico e colaboração do fornecedor Google, o qual oferece, de forma nativa, vários recursos de segurança, pois atendem a diversas 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 ajuda a proteger contra *malware* e vírus desconhecidos, entre outros recursos de segurança embarcados na solução.

5.15 Controle Contra Software Malicioso/ Antivírus

Os equipamentos dos colaboradores da Hub Fintech possuem a solução de proteção Antimalware , que é uma plataforma de gerenciamento centralizado de segurança para terminais físicos, máquinas virtuais e servidores. Essa ferramenta fornece visualização clara das posturas de segurança, ameaças globais e painéis de visualização com informações importantes sobre detecção, contenção e exclusão de ameaças, para correta administração do ambiente de TI.

5.16 Contingência

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

A infraestrutura possui contingência em zonas distintas, garantindo assim a disponibilidade dos sistemas utilizados pela Hub Fintech.

5.17 Planos de Continuidade de Negócios

Os planos de continuidade de negócio tem o objetivo de 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 Hub Fintech.

5.18 Classificação dos Dados e das Informações

I. **Pública:** Toda informação que pode ser exposta publicamente e possui autorização para isso como campanha publicitária, notícias publicadas, e-mail marketing e canais de comunicação oficiais;

II. **Uso Interno:** Todo dado e informação gerado, obtido, adquirido sob responsabilidade da Hub Fintech, com o intuito de orientar e/ou subsidiar a condução dos negócios e/ou atividades da Empresa, a exemplo das políticas e procedimentos, comunicados internos e e-mails de colaboradores;

III. **Uso Restrito:** Informações de uso limitado às áreas responsáveis pela produção da informação e/ou pelo seu tratamento;

IV. **Confidencial:** Todo dado ou informação financeira, contábil ou gerencial que trate de desempenho e resultados da Hub Fintech (antes de sua publicação oficial), relatórios técnicos, contratos e demais informações a respeito do Hub Fintech, parceiros de negócio e fornecedores, que tenham restrição de acesso em decorrência de determinação legal, contratual, acordo comercial, acordo de cooperação técnica, entre outros.

V. **Sigilosa:** Todos os dados e informações sobre planos estratégicos, desenvolvimento de produtos e/ou serviços, campanhas publicitárias, operações de mercado, metas, aquisição, fusões e incorporações.

Importante: O acesso, a divulgação e o tratamento de informação sigilosa ficarão restritos às pessoas que tenham necessidade de conhecê-la, sempre vinculado ao compromisso de manutenção de seu sigilo.

Nota 1: A classificação deverá ser realizada no momento em que a informação/dado for gerada ou, posteriormente, sempre que necessário.

Nota 2: Na hipótese de documento que contenha informações classificadas em diferentes tipos, será atribuído ao documento o tratamento mais rigoroso, isto é, sigilosa, ficando assegurado o acesso apenas após aprovação da Diretoria Colegiada.

6 DISPOSIÇÕES GERAIS

6.1 Aplicabilidade

Esta Política se aplica a todos os administradores, colaboradores, parceiros e fornecedores relevantes, que processem dados ou informações sensíveis por definição legal ou regulatória ou que sejam relevantes para a condução das atividades operacionais da Hub Fintech.

6.2 Exceções

Todas as exceções às diretrizes desta Política, devem ser analisadas e aprovadas pela Diretoria Colegiada da Hub Fintech.

6.3 Vigência e Aprovação

Esta política tem vigência a partir da data de sua aprovação pela Diretoria Colegiada, podendo ser revisada sempre que necessário.

6.4 Política de Consequências a Violações

As sanções à presente política serão aplicadas em conformidade com a Política de Consequências.

Os colaboradores, enquanto vigorar o regime jurídico ao qual estiverem submetidos, ou após a eventual rescisão, estão sujeitos a todas e quaisquer medidas judiciais aplicáveis em razão do ato ilícito praticado, como indenização por perda e danos, além da aplicação dos procedimentos criminais pertinentes, tais como crimes relacionados à concorrência desleal, divulgação de informações sensíveis, entre outros existentes no Código Penal Brasileiro e demais legislações aplicáveis.

As medidas de consequências adotadas pela Hub Fintech, 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 Auditoria Corporativa, em conjunto com a área de Segurança da Informação e Segurança Cibernética e à Diretoria de Compliance,

Integridade e PLD conduzirem os processos de apuração dos incidentes relatados e submetê-los à Diretoria Colegiada.

7. REFERÊNCIA

- Resolução BCB nº85/2021;
- Código de Ética e Conduta;
- Código de Conduta de Fornecedores;
- Política de LGPD;
- Procedimento de Desenvolvimento Seguro;
- 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. Ou seja, não conte 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 mantenha uma solução de antivírus atualizada e instalada no computador utilizado para acesso aos serviços oferecidos pela Hub Fintech.

Adicionalmente deve 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 mesmo 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 empresa, 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*

Técnica utilizada por cibercriminosos para enganar os usuários, através de envio de *e-mails* maliciosos, para obter informações pessoais como senhas, nº de cartão de crédito, nº 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

São *e-mails* não solicitados, os quais 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 em Celular

- Não utilize aparelhos de outras pessoas para acessar aos serviços da Hub, 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.