POLÍTICA

Segurança da Informação

(PSI)

Departamento Emitente: Segurança da Informação	Responsável: Issami Suzuqui
Número / versão: Política de Segurança da Informação - v01/2020	Aprovação: Presidência - Alexandre Brito
Data: 27/07/2020	Pagina: 1 de 15

Sumário

1. OBJETIVO

Esta Política tem como objetivo estabelecer conceitos, diretrizes e responsabilidades sobre os principais aspectos relacionados à segurança da informação, visando preservar a confidencialidade, integridade, disponibilidade e conformidade de todas as informações sob gestão da Hub Fintech. Definir os princípios fundamentais que formam a base da Política de Segurança da Informação (PSI), norteando a elaboração de políticas, processos, padrões e procedimentos.

2. ABRANGÊNCIA

Esta Política abrange todas as áreas da Hub Fintech.

3. ÁREA RESPONSÁVEL

Segurança da Informação.

4. TERMOS E DEFINIÇÕES

Ameaça: qualquer causa potencial de um incidente indesejado que possa resultar em impacto nos objetivos do negócio. As ameaças podem ser internas ou externas, intencionais ou não intencionais.

Boas Práticas de Segurança da Informação: são consideradas boas práticas de segurança da informação as recomendações contidas em políticas e instituições como: ISO/IEC 27002, ISO/IEC 27001, ISO/IEC 31000, OWASP (www.owasp.org), NIST (www.nist.gov), SANS (www.sans.org) e outras internacionalmente reconhecidas.

Colaborador: entende-se como colaborador qualquer pessoa que trabalhe para a Hub Fintech, quer seja com registro em carteira de trabalho, aprendiz ou *trainee*.

Controle: qualquer recurso ou medida que assegure formas de tratamento de riscos, incluindo a redução, eliminação ou transferência. A implantação e manutenção adequada de controles materializa a segurança das informações. Podem ser interpretados como controles: políticas, processos, estruturas organizacionais, técnicas padrões, *software*, *hardware* e outros.

Gestor: colaborador que exerce cargo de liderança, como: Presidente, Vice-Presidente, Diretor, Gerente, Coordenador, Líder ou Chefe de Seção.

Informação: qualquer conjunto organizado de dados que possua algum propósito e valor para a Hub Fintech, seus clientes, parceiros e colaboradores. A informação pode ser de propriedade da empresa, estar sob sua custódia ou sob custódia de terceiros.

Prestador de Serviço: a prestação de serviço é entendida como a realização de trabalho oferecido ou contratado por terceiros (comunidade ou empresa), incluindo assessorias, consultorias e cooperação interinstitucional. A prestação de serviço se caracteriza pela intangibilidade, inseparabilidade (produzido e utilizado ao mesmo tempo) e não resulta na posse de um bem.

Princípios de "*Least Privilege" e "Need to Know*": esses princípios devem reger a autorização de qualquer acesso a sistemas e informações. Segundo eles, deve ser concedido apenas o nível mínimo de acesso (*Least Privilege*) a quem realmente tenha a necessidade de acesso (*Need to Know*).

PSI (Políticas de Segurança da Informação): estrutura de documentos internos formada por diretrizes e padrões de segurança da informação, publicados na empresa para que sejam seguidos por todos os colaboradores.

Recursos: quaisquer recursos, tangíveis ou intangíveis, pertencentes a serviço ou sob responsabilidade da Hub Fintech, que possuam valor para a empresa. Podem ser considerados recursos: pessoas, ambientes físicos, tecnologias, serviços contratados em nuvem, sistemas e processos.

Risco: qualquer evento que possa afetar a capacidade da companhia de atingir seus objetivos e suas estratégias de negócio ou, conforme a ISO 31000, o efeito da incerteza nos objetivos.

Segurança da Informação (SI): segurança da informação é a proteção das informações, sendo caracterizada pela preservação de:

- **Confidencialidade**: garantia de que a informação somente será acessada por pessoas efetivamente autorizadas;
- **Integridade**: garantia de que a informação somente será modificada por pessoas efetivamente autorizadas a fazê-lo e dentro dos métodos aprovados para estas ações;
- **Disponibilidade**: garantia de que os colaboradores autorizados obtenham acesso à informação e aos sistemas correspondentes sempre que necessário, nos períodos e ambiente aprovado pela empresa;

- **Conformidade**: garantia de que controles de segurança da informação, devidamente estabelecidos, estão sendo executados conforme esperado e produzindo resultados efetivos no cumprimento de seus objetivos.
- **Dado Pessoal**: informação relacionada a pessoa natural identificada ou identificável;
- **Titular:** pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;
- **Controlador:** pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
- **Operador:** pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

5. DIRETRIZES

Segurança da informação é a proteção das informações contra diversos tipos de ameaças, para minimizar a exposição da empresa a riscos, garantindo que as características fundamentais da informação sejam preservadas, sendo elas:

- Confidencialidade;
- Integridade;
- Disponibilidade;
- Conformidade.

Isso significa proteger a empresa contra o vazamento de informações, contra fraudes, zelar pela privacidade, garantir que sistemas e informações estejam disponíveis quando necessário e zelar pela proteção da imagem e das marcas da empresa.

A Hub Fintech, por meio de seu departamento de Segurança da Informação e de forma alinhada com os objetivos e requisitos do negócio, estabelecem nesta Política de Segurança da Informação, regras e direcionamentos a serem seguidos e aplicados às pessoas, processos e tecnologia, de forma a proteger as informações da Hub Fintech, de seus clientes, fornecedores e parceiros de negócios.

A informação é um ativo essencial para os negócios de uma organização e, sendo assim, deve ser adequadamente protegida.

5.1. Aquisição, Desenvolvimento e Manutenção de Tecnologia da Informação

Aquisições, desenvolvimento, contratações e a manutenções de tecnologia da informação devem ser centralizadas e gerenciadas pela área de Tecnologia da Informação.

A área de Tecnologia da Informação, responsável pela aquisição de produtos ou serviços de tecnologia da informação, assim como o desenvolvimento e manutenção de ativos tecnológicos, deve:

- Garantir a adoção e manutenção dos padrões dos requisitos previamente definidos nos *baselines*, padrões e políticas de segurança da informação; garantir o envolvimento da área de Segurança da Informação na análise crítica de novas soluções ou para aquelas que sofreram alterações significativas;
- Garantir o atendimento aos requisitos de segurança necessários para assegurar a confidencialidade, integridade, disponibilidade e conformidade de sistemas e informações.
- Garantir que novas soluções sejam devidamente documentadas, assim como mantida documentação para entendimento e rastreabilidade das ações realizadas.

Os recursos de tecnologia da informação utilizados pela Hub Fintech devem ser inventariados, controlados e colocados à disposição de acordo com as regras de acesso vigentes e boas práticas de segurança da informação.

Na contratação de serviços, os contratos firmados entre as partes e a Hub Fintech devem conter cláusulas de confidencialidade, responsabilidade pela proteção da informação, não divulgação (não divulgação de informações) e descarte das informações. Outras cláusulas específicas de segurança da informação podem ser requeridas de acordo com o contexto do serviço contratado.

O sigilo necessário com as informações da Hub Fintech deve perdurar mesmo após o encerramento da prestação de serviços. Esse ponto deve ser previsto no estabelecimento de contratos.

A veracidade das informações contidas em contratos deve ser verificada pela área Jurídica.
Devem ser seguidas as boas práticas de segurança da informação no ciclo de desenvolvimento de sistemas da Hub Fintech

5.2. Classificação da Informação

Toda a informação deve ser classificada de acordo com seu valor, grau de sigilo, criticidade e sensibilidade perante o negócio, de forma que sejam adotados os mecanismos de proteção adequados, balanceando custo e complexidade do controle.

Informações sem classificação explícita devem ser consideradas como “interno”, não sendo permitido o seu repasse ou divulgação para qualquer pessoa que não seja da Hub Fintech, exceto informações públicas e de mercado, devidamente autorizadas.

Todos os colaboradores devem tratar as informações da Hub Fintech, 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 e disponibilidade da Hub Fintech.

5.3. Comportamento Seguro

Os recursos e as informações de propriedade ou sob custódia da Hub Fintech devem ser utilizados de acordo com os interesses da organização, para prestação dos seus serviços, atendendo aos requisitos e respeitando as regras estabelecidas.

Independente dos meios onde à informação esteja armazenada ou transmitida, cada colaborador deve assumir um comportamento seguro e proativo impedindo seu vazamento para pessoas ou meios externos da Hub Fintech.
Aos colaboradores, sem autorização prévia, é vetado emitir opiniões em nome da Hub Fintech ou utilizar informações privadas em *e-mails*, *sites*, redes sociais, publicações impressas, fóruns de discussão, serviços da internet e outros ambientes públicos, em face da possibilidade de divulgação inadvertida.

O uso da marca, nome ou citação da Hub Fintech deve cumprir os requisitos de autorização por direito de imagem e propriedade.

Os colaboradores são responsáveis por manter as informações da Hub Fintech em locais seguros. Isso se aplica a informações impressas, escritas em quadros ou em outras mídias físicas, que não devem ser deixadas desprotegidas em salas de reuniões, mesas ou qualquer local dentro e fora da empresa.

O descarte de informações internas, restritas ou confidenciais contidas em qualquer meio, quer seja impresso, eletrônico, magnético, ou sob qualquer outra forma, deve ser feito de forma segura, garantindo a destruição dos dados de forma que não possam ser novamente recuperados.

O uso de recursos tecnológicos para gravação, foto e filmagem de qualquer reunião ou evento corporativo não é permitido sem prévia autorização e consentimento de todos os participantes.

5.4. Conformidade

O cumprimento e aderência às leis, regulamentações, Políticas de Segurança da Informação, obrigações contratuais, e padrões de segurança, são obrigatórios e devem ser garantidos por todos os colaboradores.

Responsáveis por recursos críticos da Hub Fintech devem garantir a retenção de evidências da execução de seus controles, para fornecimento em casos de auditorias ou necessidade do atendimento a regulamentações.

5.5. Conscientização e Divulgação de Segurança da Informação

A diretriz de segurança da informação e padrões de segurança devem ser amplamente divulgadas no processo de admissão e integração de novos colaboradores, tanto pelas equipes de Recursos Humanos, quanto pelos Gestores.

Todos os programas de conscientização de segurança da informação devem estar alinhados com a área de Segurança da Informação. A divulgação e reciclagem das políticas de segurança da informação devem ser estabelecidas e praticadas regularmente, de forma a garantir que todos os colaboradores conheçam as diretrizes e suas responsabilidades.

5.6. Continuidade de Negócios

Deve-se estabelecer, documentar, implantar e manter processos, procedimentos e controles, para assegurar o nível requerido de continuidade para os serviços e processos de negócio da Hub Fintech, durante situações adversas.

5.7. Segurança Física

O acesso físico a sede da Hub Fintech e as áreas restritas deve ser permitido apenas aos colaboradores ou visitantes que estejam portando crachá em local visível, sendo controlado por catracas ou outros dispositivos de controle eletrônico de acesso. Na ausência de controles automatizados o responsável pela área deve garantir que o controle seja realizado de forma pessoal, por meio da verificação do porte de crachás por colaboradores e visitantes. Nenhum visitante tem a autorização de circular pelas dependências da companhia sem estar acompanhado por um colaborador da Hub Fintech.

A identificação e registro de pessoas e equipamentos são obrigatórios, seguindo o procedimento definido pela área de Riscos.

As recepções e áreas de maior criticidade devem estar sob proteção de um circuito interno de câmeras de vídeo, instaladas em locais estratégicos. Nas referidas áreas haverá sinalização informando sobre o uso de câmeras de vídeo. As imagens obtidas devem ser preservadas com segurança.

5.8. Acesso Lógico

O processo de gestão dos acessos a qualquer sistema da Hub Fintech quer seja interno ou em nuvem, deve ser conduzido pelo departamento de Tecnologia da Informação. Exceções deverão ser tratadas junto ao departamento de Segurança da Informação.

O acesso a qualquer sistema tecnológico da Hub Fintech deve ser autenticado, ou seja, protegido por credenciais de acesso, certificados, *tokens* ou qualquer outro método seguro de identificação e autenticação.

Acessos a informações e a sistemas da Hub Fintech devem ser permitidos apenas após dois ou mais níveis de autorização, sendo o primeiro do Gestor do colaborador solicitante e o segundo do responsável pela informação ou sistema.

Os acessos de colaboradores devem ser desativados assim que desligados ou encerrados contratos de prestação de serviços.

As credenciais de acesso a sistemas e informações compostas por usuário e senha são concedidas pela Hub Fintech aos colaboradores para uso em atividades relacionadas ao seu trabalho, enquanto perdurar seu vínculo com a empresa.

É proibido transferir, compartilhar, emprestar ou revelar a senha das credenciais de acesso concedidas pela empresa a outros colaboradores, assim como é proibido o uso de credenciais de outros colaboradores.

Todos os perfis de usuários e acessos a informações ou sistemas de média e alta criticidade devem ser revisados periodicamente pelo respectivo responsável, seguindo os critérios de segregação da função e observando o princípio de mínimo acesso (*least privilege*) e necessidade de conhecimento (*need to know*).

5.9. Gestão de Riscos de Segurança da Informação

A gestão de riscos de segurança da informação deve ser realizada em um processo estruturado que contemple a identificação, análise, avaliação, priorização,

comunicação, tratamento e monitoramento dos riscos que podem afetar negativamente os negócios da organização.

O processo de gestão de riscos deve contemplar novos ativos, sistemas ou processos, quer sejam eles internos, em nuvem ou conduzidos por parceiros.

5.10. Incidentes de Segurança da Informação

São considerados incidentes de segurança da informação quaisquer eventos adversos de segurança, confirmados ou sob suspeita, que levem ou possam levar ao comprometimento de um ou mais dos princípios básicos de SI: confidencialidade, integridade, disponibilidade e conformidade, colocando o negócio em risco.
Violações ou tentativas de violação desta diretriz ou de controles de segurança da informação, intencionais ou não, são considerados incidentes de segurança.

Colaboradores devem informar imediatamente a área Segurança da Informação e o encarregado de proteção de dados de todas às violações às políticas de segurança da informação e de privacidade, bem como padrões de segurança da informação, incidentes ou anomalias que possam indicar a possibilidade de incidentes, sobre os quais venham a tomar conhecimento.

Eventos de segurança da informação e de privacidade devem ser avaliados e deve ser decidido se eles podem ser classificados como um incidente de segurança da informação e de privacidade.

A identificação de incidentes de segurança pode ocasionar o bloqueio imediato dos acessos dos colaboradores envolvidos até que sejam concluídas as investigações necessárias.

O encarregado de proteção de dados ao constatar que o incidente de segurança envolva dados pessoais, deverão adotar as providências cabíveis de acordo com o procedimento adotado pela Hub Fintech.

5.11. Monitoramento

Todas as ações de colaboradores e visitantes, realizadas nas dependências da Hub Fintech ou remotamente, abrangendo o acesso físico e a utilização de recursos de tecnologia da informação e comunicação do grupo, podem ser monitoradas.

A área de Segurança da Informação é responsável por garantir a privacidade dos registros oriundos do monitoramento de acesso e uso de sistemas e serviços de Tecnologia da Informação.

Ao acessarem sistemas e recursos tecnológicos da Hub Fintech, estão cientes que os sistemas e recursos tecnológicos podem ser monitorados, devendo utilizá-los exclusivamente para fins profissionais

Os registros obtidos no monitoramento podem ser utilizados em processos de investigação de incidentes e suspeitas de violação de leis e de políticas do grupo, bem como, em processos judiciais e trabalhistas, a critério da Hub Fintech.

5.12. Privacidade

Deve-se assegurar a privacidade e a proteção, conforme previsto pela legislação e regulamentação pertinente, de todas as informações pessoais de clientes, colaboradores, parceiros de negócio e outras que venham a ser armazenadas, processadas ou colocadas sob custódia da Hub Fintech. O tratamento de dados pessoais deve seguir, com rigor, as disposições de leis pertinentes, como, mas não se limitando ao Código de Defesa do Consumidor (Lei nº 8.078/90), MCI (Marco Civil da *Internet* - Lei 13.965/2014) e a LGPD (Lei Geral de Proteção de Dados – Lei 13.709/2018), além das normas internas de privacidade e de proteção de dados.

5.13. Propriedade Intelectual

A Hub Fintech é proprietária ou custodiante responsável por toda a informação criada, armazenada, transmitida, transportada, processada ou descartada pelos seus recursos ou por aqueles contratados pela Hub Fintech em nuvem ou prestados por prestadores de serviço devidamente autorizados.

É vetada aos colaboradores a violação da propriedade intelectual da Hub Fintech ou de terceiros, quer seja por meio da utilização indevida de imagens, textos, *softwares,* marcas ou pela cópia indevida de originais ou conversão do formato desses.

5.14. Utilização de Recursos de Tecnologia da Informação

Para utilização de qualquer recurso de tecnologia da informação é necessária à aprovação prévia do Gestor do colaborador e do proprietário da informação, sistema ou recurso. Casos onde a área de Segurança da Informação identificar que possa colocar em risco as informações do grupo, deverá ser analisado e tratado.

Não é permitida aos colaboradores a instalação de qualquer *software* ou a alteração de parâmetros de configuração de computadores da Hub Fintech. Essas devem ser realizadas por equipes de TI autorizadas, após processos de homologação e obtenção do licenciamento adequado. *Softwares* instalados indevidamente poderão ser automaticamente excluídos, sem prévio aviso.

É proibido o armazenamento, transmissão, processamento e impressão de conteúdo que contenha pedofilia, pornografia, erotismo, violência, terrorismo, racismo, intolerância, e outros conteúdos proibidos por leis, moral, ética e políticas da Hub Fintech.

As informações internas, restritas e confidenciais ou sensíveis da Hub Fintech não devem ser copiadas, sincronizadas ou replicadas em serviços em nuvem, exceto situações analisadas e aprovadas por Segurança da Informação.

O acesso de celulares, *smartphones*, *tablets* e qualquer outro dispositivo a serviços e informações da Hub Fintech devem ser permitidos apenas após o atendimento integral dos requisitos de segurança da Hub Fintech definidos nas políticas para esta categoria de dispositivos.

Documentos eletrônicos de uso da Hub Fintech devem ser armazenados em repositórios centralizados da rede (servidores de arquivos) com as devidas proteções de segurança, dentre elas: controle de acesso e *backup.* Documentos eletrônicos do grupo não devem ser armazenados em estações de trabalho.

Os colaboradores devem zelar pela segurança de ativos da empresa colocados sob sua responsabilidade, como dispositivos móveis e *notebooks*.

O uso de recursos de criptografia deve ser autorizado pelo departamento de Segurança da Informação e estar de acordo com os padrões definidos pela Hub Fintech.

Quaisquer tratamentos de dados, como coleta, compartilhamento e eliminação, por meio dos recursos de tecnologia da informação da Hub Fintech, devem ser realizados em conformidade com as suas normas das políticas internas.

5.15. Aplicabilidade

O Gestor imediato ou a área de Segurança da Informação deve ser consultado sempre que existir alguma dúvida referente à aplicabilidade da diretriz de segurança da informação e demais documentos que compõe a PSI.

Cabe à área de Segurança da Informação e ao Encarregado de Proteção de Dados avaliar os riscos de ações não previstas na PSI, se necessário levando o assunto para a deliberação de um Comitê de Segurança.

Exceções às diretrizes contidas neste documento e nos demais que compõem a PSI devem ser autorizadas pelo departamento de Segurança da Informação com participação do Encarregado de Proteção de Dados.

5.16. Responsabilidades

Todo colaborador, independente do cargo, função ou local de trabalho, é responsável pela segurança das informações da Hub Fintech e deve cumprir as diretrizes descritas na política e padrões de segurança da informação.

Colaborador

- Utilizar de modo seguro, responsável, moral e ético, todos os serviços e sistemas de TI que lhe forem concedidos;
- Notificar a área de Segurança da Informação sobre as violações das políticas contidas no PSI e sobre os eventuais incidentes ou indícios de incidentes de segurança e de privacidade que venha a tomar conhecimento;
- Manter o sigilo das informações que tenha obtido acesso enquanto colaborador da Hub Fintech, mesmo após seu desligamento da empresa.

Gestor

- Apoiar e incentivar o estabelecimento da PSI na empresa;
- Garantir que seus subordinados tenham acesso e conhecimento desta Política e demais diretrizes e padrões de segurança da informação e de privacidade;
- Fornecer os recursos financeiros, técnicos e humanos necessários para desenvolver, implantar, manter e aprimorar a segurança das informações da Hub Fintech;
- Avaliar periodicamente o grau de sigilo e segurança necessários para a proteção das informações sob sua responsabilidade e de sua equipe;
- Designar mais de um responsável para atuação em processos e operações suscetíveis a fraudes, tomando os devidos cuidados para preservar a segregação de funções;
- Autorizar acessos de seus colaboradores apenas quando forem realmente necessários, segundo os conceitos de *need to know e least privilege*.

Área de Segurança da Informação

- Orientar e coordenar as ações de segurança da informação, promovendo a execução de acordo com o que foi estabelecido;
- Desenvolver e estabelecer programas de conscientização e divulgação da PSI;
- Conduzir o processo de gestão de riscos de segurança da informação;
- Conduzir a gestão de incidentes de segurança da informação, incluindo as investigações para determinação de causas e responsáveis e a comunicação dos fatos ocorridos;
- Conduzir os processos de monitoramento e segurança da informação;
- Definir controles para tratamento de riscos, vulnerabilidades, ameaças e não conformidades identificadas pelos processos de SI;
- Propor projetos e iniciativas para melhoria do nível de segurança das informações da Hub Fintech.

Área Tecnologia da Informação (TI)

- Manter atualizada a infraestrutura tecnológica, de acordo com a recomendação de fabricantes de *hardware* e *software*;
- Tratar os riscos e vulnerabilidades identificados em ativos, sistemas ou processos sob sua responsabilidade ou custódia;
- Conduzir a gestão dos acessos a sistemas e informações da Hub Fintech;
- Implantar e manter funcionais os controles e padrões de segurança definidos para os ativos de tecnologia;
- Informar imediatamente a área de Segurança de Informação, sobre violações, falhas, anomalias, vulnerabilidades e outras condições que possam colocar em risco as informações e ativos da Hub Fintech ou dados pessoais;
- Controlar alterações em ativos de TI e garantir que estas sejam analisadas criticamente e testadas, para que não ocorram impactos adversos na operação da empresa ou em sua segurança;
- Garantir a continuidade dos serviços tecnológicos de forma a atender aos requisitos essenciais do negócio e à proteção de dados pessoais.
- Garantir que todos os ativos críticos de tecnologia da informação sejam instalados em ambientes especializados conhecidos como *Data Centers*. Esses devem conter todas as proteções e contingências necessárias para a sua respectiva proteção.

Recursos Humanos

- Verificar o histórico de candidatos a emprego, de acordo com a ética e leis vigentes;
- Garantir que a Política de Segurança da Informação e seus procedimentos sejam seguidos e divulgados no processo de admissão/integração de novos colaboradores.

Área Jurídica

- Apoiar na aplicação de medidas disciplinares referente às violações da política de segurança da informação e de Privacidade;
- Identificar requisitos legais pertinentes à segurança da informação e à privacidade;
- Garantir a adoção de cláusulas pertinentes à segurança das informações e à proteção de dados nos contratos estabelecidos com a Hub Fintech.

Riscos

- Monitorar o acesso físico de colaboradores às instalações da Hub Fintech;
- Administrar o controle de acesso físico.

Fornecedores e Parceiros de Negócios

- Cumprir as determinações das Políticas e Procedimentos publicados pela Hub Fintech;
- Orientar os colaboradores da empresa sobre o cumprimento das determinações das diretrizes e Procedimentos publicados pela Hub Fintech;
- Cumprir com o acordo de confidencialidade.

Observação

No caso de prestadores de serviço (terceiros), pode ser solicitada às suas respectivas empresas, a troca da equipe alocada na Hub Fintech, ou ainda, podem ser aplicadas penalidades a empresa tais como: multas, cancelamento do contrato e ações judiciais.