

hub

f i n t e c h

POLÍTICA DE SEGURANÇA CIBERNÉTICA



Sumario

| | | |
|--------|---|----|
| 1 | – OBJETIVO | 3 |
| 2 | – VIGÊNCIA | 3 |
| 3 | – PRINCÍPIO DE SEGURANÇA DA INFORMAÇÃO..... | 3 |
| 4 | – INFORMAÇÕES CONFIDENCIAIS..... | 4 |
| 5 | – ESTRUTURA DE GERENCIAMENTO DE SEGURANÇA CIBERNÉTICA | 5 |
| 5.1 | – Gestão de acessos às informações | 5 |
| 5.2 | – Proteção do ambiente..... | 6 |
| 5.2.1 | – Autenticação | 6 |
| 5.2.2 | – Gestão de Incidentes de Segurança da Informação..... | 7 |
| 5.2.3 | – Prevenção a Vazamento de Informações..... | 7 |
| 5.2.4 | – Testes de Intrusão | 7 |
| 5.2.5 | – Varredura de Vulnerabilidades | 7 |
| 5.2.6 | – Controle conta Software Malicioso..... | 7 |
| 5.2.7 | – Criptografia..... | 8 |
| 5.2.8 | – Rastreabilidade | 8 |
| 5.2.9 | – Segmentação de Rede..... | 8 |
| 5.2.10 | – Desenvolvimento Seguro | 9 |
| 5.2.11 | – Cópias de Segurança (Backup) | 9 |
| 5.3 | – PROCESSAMENTO, ARMAZENAMENTO DE DADOS E COMPUTAÇÃO EM NUVEM | 9 |
| 6 | – PRINCIPAIS RECOMENDAÇÕES DE SEGURANÇA AOS CLIENTES e USUÁRIOS | 10 |
| 6.1 | – Autenticação e Senha..... | 10 |
| 6.2 | – Antivírus..... | 10 |
| 6.3 | – ENGENHARIA SOCIAL..... | 11 |
| 6.3.1 | – Phishing..... | 11 |
| 6.3.2 | – SPAM | 12 |
| 6.3.3 | – FALSO CONTATO TELEFÔNICO | 12 |
| 7 | – COMUNICAÇÃO | 12 |
| 8 | – CONTROLE DAS REVISÕES..... | 12 |

1 – OBJETIVO

A Política de Segurança Cibernética (“Política”) da Hubfintech visa garantir a proteção, a manutenção da privacidade, integridade, disponibilidade e confidencialidade das informações de sua propriedade e/ou sob sua guarda, além de prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados com o ambiente cibernético, definindo as regras que representam, em nível estratégico, os princípios fundamentais incorporados para o alcance dos objetivos de segurança da informação.

Essa Política demonstra o compromisso da Hubfintech e de sua Alta Administração em zelar e tratar as informações de seus clientes, de forma a proporcionar plena satisfação quanto à segurança e privacidade de suas informações. Demonstramos também o nosso compromisso com os aspectos regulatórios e estratégicos da empresa, estando assim, em conformidade com as principais regulamentações vigentes.

2 – VIGÊNCIA

Esta Política pode ser revisada anualmente ou, quando necessário, caso haja alguma mudança nas normas da Hubfintech, alteração de diretrizes de segurança da informação, objetivos de negócio ou se requerido pelo regulador local.

3 – PRINCÍPIO DE SEGURANÇA DA INFORMAÇÃO

Consideramos que os ativos de informação são os bens mais importantes no mercado financeiro,

portanto, tratá-los com responsabilidade é o nosso compromisso. Dessa forma, estamos fundamentados nos princípios de segurança da informação, cujo objetivos constituem a preservação da propriedade da informação, notadamente sua confidencialidade, integridade e disponibilidade, permitindo o uso e compartilhamento de forma controlada, bem como o monitoramento e tratamento de incidentes provenientes de ataques cibernéticos.

Confidencialidade: garantir que as informações tratadas sejam de conhecimento exclusivo de pessoas especificamente autorizadas;

Integridade: garantir que as informações sejam mantidas íntegras, sem modificações indevidas – acidentais ou propositais;

Disponibilidade: garantir que as informações estejam disponíveis a todas as pessoas autorizadas a tratá-las.

4 – INFORMAÇÕES CONFIDENCIAIS

O acesso às informações confidenciais, incluindo dados pessoais, coletadas e armazenadas pela Hubfintech é restrito aos profissionais autorizados ao uso direto dessas informações, e necessário à prestação de seus serviços, sendo limitado o uso para outras tarefas, devendo respeitar, ainda, o disposto na Norma de Classificação da Informação.

A Hubfintech poderá revelar as informações confidenciais nas seguintes hipóteses:

- Sempre que estiver obrigado a revelá-las, seja em virtude de dispositivo legal, ato de autoridade competente, ordem ou mandado judicial;

- Aos órgãos de proteção e defesa de crédito e prestadores de serviços autorizados pela Hubfintech a defender seus direitos e créditos;
- Aos órgãos reguladores do mercado financeiro; e
- Para outras instituições financeiras, desde que dentro dos parâmetros legais estabelecidos para tanto, podendo, nesta hipótese, o usuário, a qualquer tempo, cancelar sua autorização.

5 – ESTRUTURA DE GERENCIAMENTO DE SEGURANÇA CIBERNÉTICA

O gerenciamento dos controles de segurança objetiva assegurar que os procedimentos operacionais sejam desenvolvidos, implantados e mantidos ou modificados de acordo com os objetivos estabelecidos nesta Política.

5.1 – Gestão de acessos às informações

Os acessos às informações são controlados, monitorados, restringidos à menor permissão e privilégios possíveis, revistos periodicamente, e cancelados tempestivamente ao término do contrato de trabalho do colaborador ou do prestador de serviço.

Os equipamentos e instalações de processamento de informação crítica ou sensível são mantidos em áreas seguras, com níveis de controle de acesso apropriados, incluindo proteção contra ameaças físicas e ambientais.

Os colaboradores e terceiros da Hubfintech são treinados, periodicamente, sobre os conceitos de segurança da informação, através de um programa de conscientização e disseminação da cultura de segurança cibernética.

5.2 – Proteção do ambiente

São constituídos controles e responsabilidades pela gestão e operação dos recursos de processamento das informações, visando garantir a segurança na infraestrutura tecnológica por meio de um gerenciamento efetivo no monitoramento, tratamento e na resposta aos incidentes, com o intuito de minimizar o risco de falhas e a administração segura de redes de comunicações.

5.2.1 – Autenticação

O acesso às informações e aos ambientes tecnológicos deve ser permitido apenas às pessoas autorizadas pelo Proprietário da Informação, levando em consideração o princípio do menor privilégio, a segregação de funções conflitantes e a classificação da informação.

O controle de acesso aos sistemas deve ser formalizado e contemplar, no mínimo, os seguintes controles:

- A utilização de identificadores (credencial de acesso) individualizados, monitorado e passíveis de bloqueios e restrições (automatizados e manuais);
- A remoção de autorizações dadas a usuários afastados ou desligados, ou ainda que tenham mudado de função; e
- A revisão periódica das autorizações concedidas.

5.2.2 – Gestão de Incidentes de Segurança da Informação

O comportamento de possíveis ataques é identificado 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.

5.2.3 – Prevenção a Vazamento de Informações

Utilização de controle para prevenção de perda de dados, responsável por garantir que dados confidenciais não sejam perdidos, roubados, mal utilizados ou vazados na web por usuários não autorizados.

5.2.4 – Testes de Intrusão

Testes de Intrusão interno e externo nas camadas de rede e aplicação devem ser realizados no mínimo anualmente.

5.2.5 – 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.

5.2.6 – Controle contra Software Malicioso

Todos os ativos (computadores, servidores, etc.) que estejam conectados à rede corporativa ou façam uso de informações da Hubfintech, devem, sempre que compatível, ser protegidos com

uma solução anti-malware determinada pela área de Segurança da Informação.

5.2.7 - Criptografia

Toda solução de criptografia utilizada na Hubfintech deve seguir as regras de Segurança da Informação e os padrões de segurança dos Órgãos reguladores.

5.2.8 - Rastreabilidade

Trilhas de auditoria automatizadas devem ser implantadas para 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.

5.2.9 – Segmentação de Rede

- Computadores conectados à rede corporativa não devem ser acessíveis diretamente pela Internet;
- Não é permitida a conexão direta de rede de terceiros utilizando-se protocolos de controle remoto aos servidores conectados diretamente na rede corporativa;
- Para solicitação de criação, alteração e exclusão de regras nos firewalls e ativos de rede, o requisitante deve encaminhar pedido à área de SI, que fará a análise e aprovação, enviando para que seja executada pela área de TI.

5.2.10 – Desenvolvimento Seguro

A Hubfintech 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.

5.2.11 – Cópias de Segurança (Backup)

O processo de execução de backups é realizado, periodicamente, nos ativos de informação da empresa, de forma a evitar ou minimizar a perda de dados diante da ocorrência de incidentes.

5.3 – PROCESSAMENTO, ARMAZENAMENTO DE DADOS E COMPUTAÇÃO EM NUVEM

Conforme a Resolução 4.658/2018 (e sua alteração 4.752/2019), do Conselho Monetário Nacional, para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem, a Hubfintech assegura-se de um procedimento efetivo para a aderência às regras previstas na regulamentação em vigor.

6 – PRINCIPAIS RECOMENDAÇÕES DE SEGURANÇA AOS CLIENTES e USUÁRIOS

6.1 – Autenticação e 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 lugar algum. Ou seja, não contar a ninguém e não anotar em papel;
- Alterar a senha sempre que existir qualquer suspeita do comprometimento dela;
- Elaborar senhas de qualidade, de modo que sejam complexas e de difícil adivinhação;
- Impedir o uso do seu equipamento por outras pessoas, enquanto este estiver conectado/ "logado" com a sua identificação;
- Bloquear sempre o equipamento ao se ausentar.
- Sempre que possível, habilitar um segundo fator de autenticação (Por exemplo:SMS, Token e etc.).

6.2 – Antivírus

Recomendamos que o cliente mantenha uma solução de antivírus atualizada e instalada no computador utilizado para acesso aos serviços oferecidos pela Hubfintech.

Além disso, possuir o sistema operacional atualizado com as últimas atualizações realizadas.

6.3 – ENGENHARIA SOCIAL

Recomendamos que o cliente mantenha uma solução de antivírus atualizada e instalada no computador utilizado para acesso aos serviços oferecidos pela Hubfintech. Além disso, possuir o sistema operacional atualizado com as últimas atualizações realizadas.

6.3.1 – Phishing

Técnica utilizada por cibercriminosos para enganar os usuários, através de envio de e-mails maliciosos, afim de obter informações pessoais como senhas, cartão de crédito, CPF, número de contas bancárias, entre outros. As abordagens dos e-mails de phishing podem ocorrer das seguintes maneiras:

- Quando procuram atrair as atenções 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;

6.3.2 - 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.

6.3.3 - 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.

7 - COMUNICAÇÃO

Quaisquer indícios de irregularidades no cumprimento das determinações desta Política serão alvo de investigação interna e devem ser comunicadas imediatamente aos nossos canais de atendimento.

8 – CONTROLE DE REVISÕES

| Versão | Data atualização | Autor | Resumo das modificações |
|---------------|-------------------------|--------------------------|--------------------------------|
| V01 | 12/05/2021 | Lucas Alexandre da Silva | Criação |