Política de Segurança Cibernética

Sumário

1. OBJETIVO

O presente documento visa estabelecer diretrizes de Segurança Cibernética para a FATHER PAYMENT TRUST ALLIANCE GESTORA DE PAGAMENTO LTDA. (também conhecida como “Father Payment®” ou “Instituição” nesta Política), assim como às suas controladas e afiliadas, se houver.

A Política de Segurança Cibernética (“Política”) abrange medidas preventivas, de detecção e redução de vulnerabilidades a incidentes relacionados ao ambiente cibernético, com objetivo de reforçar a confidencialidade, disponibilidade e integridade das informações.

A Política foi elaborada em conformidade com a legislação vigente, com especial atenção à Resolução do Banco Central do Brasil (BCB) nº 85, de 8 de abril de 2021 (“Resolução BCB nº 85”), conforme aplicável.

2. APLICABILIDADE

A presente Política aplica-se a toda e qualquer atividade realizada pela Father Payment® e por suas subsidiárias e por todos os seus respectivos colaboradores, parceiros comerciais, terceiros, prestadores de serviço e quaisquer outros que venham a contribuir com as atividades da Instituição.

3. DEFINIÇÕES

Para os fins desta Política, os termos definidos abaixo terão o seguinte significado:

- **Ameaça:** Agente que pode materializar um incidente (intencional ou acidental), resultando danos aos ativos da Instituição;
- **Ativo:** Bens (patrimônios) ou equivalentes, tangíveis ou intangíveis, os quais tenham valor para a Instituição;
- ***Cloud* (Nuvem):** Rede integrada na internet que oferece serviços de tecnologia com manutenção e recursos terceirizados;
- **Colaborador:** Pessoa física que presta serviço para a Instituição e que possui vínculo empregatício;
- **Evento:** Acontecimento que acarreta mudança do estado atual de um processo;
- **Fornecedor:** Pessoa Jurídica que fornece insumos de qualquer natureza, sejam eles serviços ou produtos os quais são necessários para a Instituição realizar suas atividades;
- **Incidente:** Qualquer evento que não faz parte da operação normal de um serviço e que pode causar interrupção de serviços ou redução de sua qualidade;

- ***Malware***: É qualquer software intencionalmente feito para causar danos a um computador, servidor ou a uma rede de computadores;

- **Prestador de Serviço:** Pessoa física ou jurídica que presta serviço de qualquer natureza à Instituição;

- ***Ransomware***: É um tipo de *malware* de sequestro de dados, feito por meio de criptografia, que usa como reféns arquivos e informações, cobrando resgate para restabelecer o acesso a estas informações;

- **Risco:** Qualquer evento que possa impactar a organização e os objetivos de negócio;

- **Segurança da Informação:** Conjunto de ações que visam a preservar e garantir a disponibilidade, confidencialidade e integridade das informações pertencentes e sob a responsabilidade da Instituição, assim, mitigando os riscos e probabilidades de dano;

- **Usuário:** Colaboradores, prestadores de serviços, clientes, terceiros ou qualquer indivíduo que faça uso dos serviços prestados pela Father Payment® ou tenha acesso às informações da Instituição;

- **Vulnerabilidade:** Fragilidade que apresenta riscos potenciais que caso sejam materializados podem gerar danos à organização.

4. PRINCÍPIOS

A Father Payment® adota os seguintes princípios para guiar seus processos, implementar medidas técnicas, promover conscientização em segurança da informação e atingir os objetivos estabelecidos por essa Política. Esses princípios são:

I. **Confidencialidade:** Assegurar que toda informação será acessível apenas para pessoas autorizadas;

II. **Integridade:** Assegurar que a informação, em trânsito ou armazenada, seja completa, exata e que não sofrerá qualquer alteração ou remoção não autorizada;

III. Disponibilidade: Assegurar que a informação estará sempre disponível quando necessária.

5. DIRETRIZES

5.1. RISCOS CIBERNÉTICOS

A Father Payment® mantém uma abordagem contínua na gestão de riscos cibernéticos, visando mitigar, prevenir ou transferir eventuais riscos e suas consequências para suas operações. Essa administração é conduzida por meio de ações práticas, envolvendo o uso de ferramentas de

mercado, implementação de políticas, estabelecimento de processos e a conscientização de colaboradores, prestadores de serviços, fornecedores e clientes.

5.2. CRIPTOGRAFIA DE DADOS

A utilização de mecanismos criptográficos é fundamental para garantir a preservação da integridade e confidencialidade de dados críticos e sensíveis ao negócio. Ao empregar técnicas de criptografia de dados, a Father Payment® assegura que as informações vitais permaneçam protegidas contra acessos não autorizados, contribuindo assim para um ambiente mais seguro e confiável.

5.3. CONTROLE DE MALWARE

Os malwares, como vírus e *ransomwares*, representam ameaças significativas, podendo comprometer a integridade, confidencialidade e a disponibilidade dos dados. Dessa forma, a Father Payment® emprega medidas técnicas, por meio de ferramentas de mercado e processos robustos, para assegurar a proteção dos ambientes digitais.

5.4. CÓPIAS DE SEGURANÇA

As cópias de segurança representam uma salvaguarda essencial contra perdas de dados causadas por incidentes como falhas de *hardware*, ataques de *malware*, exclusões acidentais ou outros eventos catastróficos. Ao criar e manter cópias regularmente atualizadas dos dados, a Father Payment® garante a capacidade de restaurar informações vitais em caso de imprevistos. Isso não apenas protege contra a perda irreparável de dados valiosos, mas também contribui para a continuidade operacional, conformidade com regulamentações vigentes e assegura a confiança das partes interessadas.

5.5. PREVENÇÃO E DETECÇÃO DE INTRUSÃO

Com o intuito de aderir plenamente às diretrizes estabelecidas, a Father Payment® implementa medidas proativas que aprimoram suas defesas contra ameaças digitais. Esse comprometimento abrange a adoção de firewalls robustos, a implementação de segurança de borda, a otimização da eficácia do Centro de Operações de Segurança (SOC), a utilização de sistemas de detecção de anomalias e a manutenção constante da atualização de softwares, visando mitigar vulnerabilidades conhecidas.

5.6. GESTÃO DE ACESSOS

Os acessos físicos às instalações e dependências da Father Payment® estão sujeitos a controles rigorosos para assegurar que apenas indivíduos autorizados tenham permissão de entrada. Esse processo inclui monitoramento constante e a proteção adequada dos registros associados.

No que diz respeito aos acessos lógicos, a responsabilidade pela centralização e gestão é

da área de Segurança da Informação da Father Payment®, isso garante um controle eficaz sobre o ciclo de vida das credenciais de acesso, seguindo a premissa de conceder apenas os privilégios mínimos necessários.

5.7. VAZAMENTO DE INFORMAÇÕES

A Father Payment® adota medidas rigorosas para prevenir e mitigar potenciais vazamentos de dados. No âmbito técnico, destaca-se a utilização do *Data Loss Prevention* (DLP), cujo propósito é evitar a perda de dados decorrente de possíveis violações. Esse sistema atua por meio do monitoramento, detecção e bloqueio de dados confidenciais durante sua utilização, em trânsito ou em repouso. Além disso, o DLP abrange a proteção de dados pessoais e sensíveis, garantindo uma abordagem abrangente na segurança da informação.

5.8. AQUISIÇÃO, DESENVOLVIMENTO E MANUTENÇÃO DE SISTEMAS

Os sistemas (novo ou corrente) adquiridos pela Father Payment® passam por avaliação de risco com o objetivo de identificar possíveis fraquezas que possam impactar negativamente a informação manipulada.

No que concerne ao ciclo de desenvolvimento e na implementação de novas tecnologias, a Father Payment® garante que os controles e processos estabelecidos para identificar e corrigir vulnerabilidades sejam realizados antes que entrem em ambiente de produção.

5.9. RELACIONAMENTO COM FORNECEDORES

A Father Payment® controla o acesso dos dados organizacionais compartilhados aos fornecedores. Os fornecedores, assim como os colaboradores, apenas podem ter acesso aos dados que são necessários para executar os serviços requeridos.

Além disso, a Father Payment® possui recursos e competências necessárias para a adequada gestão dos serviços a serem contratados, inclusive para análise de informações, uso de recursos e monitoramento dos serviços a serem prestados.

5.10. SEGURANÇA NAS COMUNICAÇÕES

As transmissões das informações são protegidas com o objetivo de garantir sua segurança. Logo, as redes possuem controles implementados que asseguram que os serviços a ela conectados não sofram acessos desautorizados.

5.11. SERVIÇOS EM NUVEM

A contratação de serviços em nuvem na Father Payment® atende requisitos estipulados pelo Banco Central do Brasil e são documentados, considerando a criticidade do serviço e a sensibilidade dos dados e das informações a serem processadas, armazenadas e gerenciadas

pelo prestador de serviços em nuvem, levando em conta, inclusive, a classificação das informações.

A contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem é comunicada ao Banco Central do Brasil, informando a denominação da empresa contratada, os serviços relevantes contratados e a indicação dos países e das regiões em cada país onde os serviços poderão ser prestados e os dados armazenados, quando aplicável.

Caso a contratação de serviços relevantes de processamento, armazenamento e de computação em nuvem seja prestado no exterior, a Father Payment® garantirá o atendimento aos requisitos estipulados no Art.16 da Resolução BCB nº 85.

Quanto aos contratos para prestação de serviços relevantes de processamento, armazenamento e de computação em nuvem, contém cláusulas-padrão que atendem os requisitos estipulados no Art. 17 da Resolução BCB nº 85.

5.12. GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

O incidente de segurança da informação é toda ocorrência, confirmada ou sob suspeita, que pode comprometer a confidencialidade, integridade e disponibilidade no ambiente.

Todo incidente de segurança da informação é reportado para análise da área de Segurança da Informação e são classificados conforme sua criticidade para a continuidade do negócio, o impacto na usabilidade dos serviços e o impacto financeiro.

Em conformidade com a Resolução BCB nº 85, a Father Payment® comunicará tempestivamente ao Banco Central do Brasil as ocorrências de incidentes relevantes e das interrupções dos serviços relevantes, que configurem situação de crise pela Father Payment®, bem como das providências para o reinício das suas atividades. Além disso, disponibilizará um Relatório Anual sobre a Implementação do Plano de Ação e de Resposta a Incidentes, considerando todos os aspectos desde a identificação e a tratativa do incidente.

5.13. CONSCIENTIZAÇÃO E TREINAMENTOS

A Father Payment® se compromete a treinar e conscientizar continuamente seus colaboradores e terceiros, com o objetivo de disseminar a cultura de segurança cibernética na Instituição, como também prestar informações aos usuários, de modo geral, sobre precauções em segurança cibernética na utilização de produtos e serviços oferecidos.

Aprovado pela Diretoria da Father Payment® no dia 03.04.2024.