Requisitos de Segurança da Informação para outsourcing de ATMR

1. GERAL

1.1. A CONTRATADA se compromete a seguir os processos do CONTRATANTE no que se refere ao cumprimento das normas de segurança do CONTRATANTE, bem como se coloca à disposição para qualquer diligência técnica sempre que o CONTRATANTE julgar necessário para assegurar um risco operacional mínimo.

1.1.1. A realização de diligência será previamente agendada pelo CONTRATANTE e limitada ao ambiente e documentos relacionados com o SERVIÇO contratado.

1.2. No caso de a CONTRATADA subcontratar infraestrutura, serviços ou sistemas para a prestação dos SERVIÇOS contratados, o CONTRATANTE deve ser informado e os mesmos devem estar sujeitos as cláusulas desse contrato.

1.3. O SERVIÇO deve ser integrado de acordo com os parâmetros de segurança especificados pelo CONTRATANTE.

1.4. A CONTRATADA deve apresentar, sempre que solicitado pelo CONTRATANTE, todas as documentações de infraestrutura, arquitetura e segurança dos ambientes utilizados para a prestação do SERVIÇO.

2. EMV

2.1. Os equipamentos fornecidos e os sistemas da CONTRATADA envolvidos nas operações efetuadas pelos clientes do CONTRATANTE deverão ser capazes de efetuar o processo completo de autenticação EMV, conhecido como *full-grade*.

3. TECLADO CRIPTOGRÁFICO

3.1. Os equipamentos fornecidos deverão possuir teclado criptográfico (EPP – Encripted PINPad) homologado PCI PTS 5.x, ou superior.

3.2. O teclado criptográfico deve possuir solução contra vandalismo, com detecção de invasão e destruição das chaves em caso de violação (*Tamper Proof*).

3.3. As chaves criptográficas devem ser usadas apenas para o seu único objetivo e nunca devem ser compartilhadas entre os sistemas de produção e desenvolvimento/homologação. O teclado criptográfico deve possibilitar o armazenamento de pelo menos as chaves para criptografia de PIN e para dados.

4. CRIPTOGRAFIA ENTRE MÓDULOS

4.1. A comunicação entre a aplicação e o módulo reciclador de cédulas, leitor biométrico e placa de sensores do sistema de entintamento deve ser criptografada, a fim de impedir ataques que possibilitem, por exemplo, a dispensa e reciclagem indevida de cédulas, a execução indevida de comandos, sejam através de dispositivos espúrios, através de interferência na rede, ou através de acesso aos conectores lógicos do módulo.

5. CRIPTOGRAFIA NA COMUNICAÇÃO ENTRE CONTRATADA E CONTRATANTE

5.1. Todo o gerenciamento e o armazenamento de Chaves Criptográficas devem estar em conformidade ao estipulado nas normas “Payment Card Industry - PIN Security Requirements” e “Payment Card Industry Card Production – Logical Security Requirements”, sendo que se destacam os seguintes itens:

I. Toda chave criptográfica utilizada deve ser armazenada em HSM que esteja em conformidade com os padrões de segurança FIPS 140-2 level 3 ou 4, não sendo aceita a utilização de chaves criptográficas armazenadas em claro (plain text) em aplicação ou arquivo.

II. Todo processamento criptográfico deve ser realizado por hardware.

III. Deve haver segregação de ambientes para produção e testes, sendo que nenhuma chave criptográfica pode ser compartilhada entre os ambientes.

IV. Toda chave criptográfica deve ser destinada exclusivamente para sua finalidade, como por exemplo, chaves para proteção de PIN não podem ser utilizadas como transporte de chaves.

V. Toda chave de transporte deve ser tão forte quanto à chave que está transportando.

VI. Todo o gerenciamento de chaves criptográficas e acesso ao HSM, deve ser realizado sob duplo controle de acesso.

VII. Deve haver trilhas de auditoria que documentem todo o acesso físico e lógico ao HSM.

VIII. Deve haver processos documentados referentes ao gerenciamento de chaves criptográficas, bem como de manutenção dos dispositivos criptográficos.

5.2. Deve haver mecanismos que permitam a troca de chaves criptográficas, seja por algum comprometimento ou por entendimento do CONTRATANTE.

5.3. O CONTRATANTE pode solicitar formalmente, a qualquer momento, que a CONTRATADA destrua chaves criptográficas especificadas e a CONTRATADA deve apresentar documento registrando o processo de destruição.

5.4. A CONTRATADA deve possuir documentos descrevendo o Plano de Continuidade de Negócio, referente ao comprometimento de chaves criptográficas ou a perda de chaves.

5.5. O CONTRATANTE pode solicitar, a qualquer momento, a apresentação de documentos e evidências referentes ao objeto do Contrato, como processos criptográficos, gerenciamento de chaves, Plano de Continuidade de Negócio de chaves criptográficas, inclusive trilhas de auditoria relacionados a eventos e incidentes.

5.6. Para o processo de troca de chaves criptográficas entre as instituições, a CONTRATADA deve seguir o processo de cerimonial de inserção de chaves a ser fornecido posteriormente pelo BANRISUL. Este processo deverá ser executado na presença dos representantes do CONTRATANTE (custodiantes).

5.7. O cerimonial de inserção de chaves deve acontecer no ambiente da CONTRATADA. Este ambiente deve atender aos seguintes requisitos:

I. Possuir acesso restrito, sob controle duplo de acesso.
II. Possuir trilhas de auditoria registrando os acessos.
III. Possuir monitoração por CFTV.
IV. O CFTV não deve possibilitar a visualização dos componentes a serem digitados.
V. Possuir mecanismos que impeçam a visualização dos componentes digitados por outras pessoas que não sejam o custodiante do componente.
VI. Deverá ser aprovado pelo CONTRATANTE.

6. INTEGRAÇÃO

6.1. A comunicação entre a SOLUÇÃO e outros softwares, assim como a comunicação entre eventuais componentes da SOLUÇÃO, deverá ser sempre autenticada.

6.2. Caso sejam instalados componentes da SOLUÇÃO no ambiente do CONTRATANTE, a comunicação destes componentes com sistemas do CONTRATANTE ou outros softwares instalados no ambiente do CONTRATANTE deverá ser autenticada utilizando padrões acordados entre as partes.

6.3. Caso sejam instalados componentes da SOLUÇÃO no ambiente do CONTRATANTE, a comunicação destes componentes com softwares instalados fora do ambiente interno do CONTRATANTE deverá ser autenticada de acordo com a criticidade das informações trafegadas. O CONTRATANTE poderá exigir ajustes na autenticação em casos que considerar inseguros.

6.4. Caso haja integração de componentes da SOLUÇÃO hospedados fora do ambiente do CONTRATANTE com sistemas do CONTRATANTE, as comunicações devem ser realizadas por APIs REST, de acordo com os subitens abaixo.

6.4.1. No caso de uso de APIs fornecidas pela CONTRATADA e consumidas por sistemas internos do CONTRATANTE, as APIs devem suportar autenticação através do protocolo OAuth 2.0, conforme RFC 6749, com os seguintes requisitos:

6.4.1.1. O *endpoint* de geração de token deve:

6.4.1.1.1. Aceitar *payload* com *content-type "application/x-www-form-urlencoded"*.

6.4.1.1.2. Retornar o *payload* conforme a RFC 6749, incluindo obrigatoriamente o parâmetro "*expires_in*" e parâmetro "*token_type*" do tipo "*Bearer*".

6.4.1.1.3. Utilizar o fluxo de *client_credentials*, empregando um dos seguintes métodos de autenticação:

6.4.1.1.3.1. *client_secret_basic*, conforme RFC 6749 e RFC 7591;

6.4.1.1.3.2. *client_secret_post*, conforme RFC 6749 e RFC 7591;

6.4.1.1.3.3. *client_secret_jwt*, conforme RFC 7523 e OpenID Connect Core;

6.4.1.1.3.4. *private_key_jwt*, conforme RFC 7523 e OpenID Connect Core;

6.4.1.1.3.5. *tls_client_auth*, conforme RFC 8705.

6.4.1.2. A API deve fornecer um endpoint de metadados do servidor de autorização, de acordo com a RFC 8414, fornecendo no mínimo o token endpoint.

6.4.1.3. Os endpoints de consumo das APIs devem receber o *access token* no *header* "*Authorization*" no formato "*Bearer [access_token]*", conforme a RFC 6750.

6.4.1.4. Qualquer alteração nos protocolos e/ou parâmetros de autenticação deverá ser comunicada com no mínimo 60 dias de antecedência.

6.4.1.4.1. A CONTRATADA deverá disponibilizar versão de testes das APIs com as alterações para o CONTRATANTE verificar a conectividade antes da alteração em produção.

6.4.2. Caso sejam necessárias APIs hospedadas no ambiente do CONTRATANTE, a comunicação com estas APIs deverá ser controlada pelo gerenciador de APIs do CONTRATANTE. Os protocolos, parâmetros e métodos utilizados serão definidos pelo CONTRATANTE.

6.5. Caso haja necessidade de troca de arquivos entre a SOLUÇÃO e os sistemas do CONTRATANTE, a troca de arquivos deverá ser feita através da solução de Troca Eletrônica de Arquivos do CONTRATANTE.

7. INCIDENTES CIBERNÉTICOS

7.1. A CONTRATADA deverá possuir equipe para Resposta a Incidentes de Segurança da Informação, ou equivalente, com disponibilidade de atendimento ao CONTRATANTE 24 horas por dia, 7 dias por semana, e manter atualizados os contatos para atendimento telefônico e por e-mail.

7.1.1. A CONTRATADA deverá informar o nome do profissional responsável pela área de Segurança da Informação, ou equivalente, e seus contatos telefônico e de e-mail.

7.2. A CONTRATADA deve reportar, em 24 horas, quaisquer incidentes de segurança ou situação de segurança cibernética que possam afetar a prestação do SERVIÇO contratado e/ou os dados do CONTRATANTE, através de canal definido pelo CONTRATANTE

7.2.1. Devem ser fornecidas as evidências e informações necessárias para os processos de investigação, proteção, monitoramento e outras que o CONTRATANTE solicitar.

7.3. A CONTRATADA deve possuir procedimentos documentados para Resposta a Incidentes Cibernéticos, cuja documentação deverá ser apresentada ao CONTRATANTE sempre que solicitado.

7.4. O CONTRATANTE pode repassar as informações recebidas para Órgãos Reguladores, Órgãos Fiscalizadores e Auditorias Externas.

8. FRAUDES

8.1. A CONTRATADA será responsável pela segurança lógica dos equipamentos, incluindo a proteção do sistema e a detecção de dispositivos maliciosos instalados por terceiros para captura de informações de clientes do CONTRATANTE, como dispositivos de *skimming* ou câmeras, por exemplo.

8.2. A CONTRATADA deverá arcar com os custos e prejuízos causados por ataques efetuados ao sistema dos equipamentos.

8.3. Em caso de suspeitas e/ou incidentes de comprometimento na segurança dos equipamentos fornecidos, a CONTRATADA deverá fornecer todas as informações necessárias para a investigação e resposta do CONTRATANTE, incluindo ao menos os registros dos pontos de comprometimento e dos clientes que efetuaram operações nestes equipamentos.

8.4. Em caso de fraudes ocorridas em contas de clientes do CONTRATANTE, a CONTRATADA deverá ressarcir o CONTRATANTE caso seja comprovado que a fraude ocorreu devido a falhas na segurança dos seus equipamentos, mesmo que a transação não tenha ocorrido em um equipamento da CONTRATADA.

9. TEMPLATES DE CÉDULAS

9.1. A atualização de templates de cédulas é responsabilidade da CONTRATADA, ficando essa responsável por eventuais fraudes envolvendo cédulas falsas.