ANEXO I - ESPECIFICAÇÕES TÉCNICAS

1. CARACTERÍSTICAS GERAIS

1.1. Os equipamentos a serem fornecidos devem ser do tipo Máquina de Atendimento Automático - *Automatic Teller Machine* (ATM). Os ATM devem ser do tipo Terminal de Autoatendimento Múltiplo com funções de saque de cédulas, depósito de cédulas (sem envelopes), reaproveitamento de numerário e pagamento de boletos bancários com códigos de barras;

1.2. Os ATM e seus componentes devem ser novos, de primeiro uso e em perfeito funcionamento. Os ATM não devem estar listados em final de venda (*end-of-sale*), fim de suporte (*end-of-support*) ou fim de vida (*end-of-life*) do fabricante;

1.3. As especificações técnicas constantes do Edital, do Contrato e seus anexos são mínimas, aceitando-se, a critério do CONTRATANTE, equipamentos e/ou componentes com especificações superiores;

1.4. O número de série de cada ATM deve ser único, afixado em local visível, na parte externa traseira do gabinete superior ou do cofre;

1.5. A logomarca do fornecedor somente poderá ser aplicada na parte traseira do equipamento;

1.6. O ATM deve atender à Norma ABNT NBR15250:2005 – Acessibilidade em Caixa de Autoatendimento Bancário e seguir os preceitos do desenho universal, visando proporcionar a sua utilização à maior quantidade de pessoas, independentemente de idade, estatura ou limitação de mobilidade ou percepção, de maneira autônoma e segura;

1.7. Deve ser apresentado na homologação do ATM, relatório emitido por organismo detentor de Certificado de Acreditação concedido pelo INMETRO, atestando que o equipamento está em conformidade com a Norma ABNT NBR 15250:2005;

1.8. O ATM deve ser compatível com o Microsoft Windows 11 Professional/Enterprise x64 e Ubuntu for desktops 24.x e derivados, não sendo admitidos a utilização de nenhum, ajuste ou outras técnicas de instalação que não sejam suportadas oficialmente pelos fabricantes desses sistemas operacionais;

1.9. Todos os componentes utilizados no ATM e seus periféricos devem apresentar compatibilidade entre si, sem gerar conflitos;

1.10. Todos os ATM devem ser entregues acompanhados de manual do usuário, impresso ou em formato digital, em língua portuguesa, contendo todas as informações do produto, instruções para instalação, configuração e operação;

1.11. Devem ser fornecidos todos os cabos e componentes requeridos para o perfeito funcionamento do ATM e seus periféricos;

1.12. O ATM deve possuir sinalizações com diferenciações por cor nos locais para manuseio dos periféricos e dispositivos, nos locais para manuseio que exigem alerta ou cuidado e nos locais de risco elétrico e/ou mecânico, entre outros, que devem ser evitados ou manuseados por técnico especializado;

1.13. Todos os ATM a serem entregues deverão ser idênticos; todos os componentes externos e internos devem ser do mesmo modelo e fabricantes ou em regime de *Original Equipment Manufacturer* (OEM);

1.14. O ATM deve ser pintado em cor única, bege claro, padrão ARPOL:

- Pó: 91320856; ou
- Líquida: 1013-4532.

1.15. O ATM e seus componentes devem possuir modelo de refrigeração eficiente de forma que não provoque o superaquecimento dos componentes internos, nem acúmulo excessivo de poeira;

1.16. O peso total do ATM, incluindo todos os seus periféricos, não deve superar 1.200 kg (um mil e duzentos quilos);

1.17. Antes da homologação definitiva, o ATM deverá ser submetido a testes de intrusão conduzidos ou supervisionados pelo CONTRATANTE, abrangendo hardware, firmware, interfaces externas, módulos críticos, sistema operacional, drivers e conectividade. O CONTRATADO deverá fornecer apoio técnico e documentação. Vulnerabilidades classificadas como críticas ou altas devem ser obrigatoriamente corrigidas antes da aceitação do equipamento;

1.18. O CONTRATADO deve cooperar com ações de inteligência cibernética conduzidas pelo CONTRATANTE, fornecendo indicadores de comprometimento (IoCs), telemetrias e informações técnicas relevantes. Os resultados de testes de intrusão, varreduras periódicas e análises de vulnerabilidades dos módulos fornecidos devem ser apresentados em relatório formal contendo achados, severidade, plano e prazo de correção, disponível para auditoria;

1.19. O CONTRATADO deve assegurar a continuidade de negócios dos equipamentos e componentes fornecidos, mantendo processos documentados de backup, restauração e recuperação operacional, incluindo procedimentos formais para tratamento de indisponibilidades. Devem ser apresentados ao CONTRATANTE evidências de testes periódicos de continuidade, contemplando cenários de falha, recuperação completa e retomada, de acordo com os requisitos de disponibilidade definidos para o canal ATM;

1.20. Os cassetes de cédulas recicláveis devem ser acomodados no cofre principal; o(s) módulo(s) de recolhimento das cédulas (depósito) podem ser instalados no compartimento intermediário.

2. SOFTWARES E APLICATIVOS

2.1. Devem ser fornecidos todos os drivers e *Application Program Interfaces* (API) necessários ao funcionamento da solução proposta bem como as respectivas documentações;

2.2. O CONTRATADO deve fornecer um SBOM (Software Bill of Materials) contendo todos os componentes de software, bibliotecas, dependências e versões utilizados no ATM, incluindo drivers, APIs, firmwares e módulos embarcados, para fins de auditoria, rastreabilidade e gestão de vulnerabilidades;

2.3. O CONTRATADO deve assegurar que todos os softwares, firmwares e componentes embarcados sejam produzidos em pipelines controlados e auditáveis, com verificação de integridade, assinaturas de cadeia de fornecimento (*build attestation*) e aderência a modelos como SLSA nível 2 ou superior. Componentes críticos devem possuir rastreabilidade completa desde a origem até sua incorporação ao ATM;

2.4. As API's a serem fornecidas pelo CONTRATADO devem ser compatíveis com o Sistema de Automação Bancária utilizado no Banco, conforme definido no (**vide ANEXO II - SOFTWARE - INTERFACE DE PROGRAMACAO.docx**) do Edital, de forma a garantir a existência de uma única versão do referido software (código fonte e executável);

2.5. Deve ser fornecido software *Text to Speech* (TTS) em português do Brasil;

2.6. Deve ser fornecida licença de uso da biblioteca de cartão que segue o padrão EMV (Europay, Mastercard e Visa), a ser integrada à solução de automação bancária do Banco, permitindo o processamento completo de *Smart Cards*, segundo a norma EMV versão 4 ou superior. Este produto será entregue para o ambiente computacional Microsoft Windows.

3. ALIMENTAÇÃO ELÉTRICA

3.1. Todo o conjunto deve funcionar com tensão elétrica nominal Full Range, entre 100V e 240V~ AC, frequência de 50/60 Hz, com seleção automática de voltagem;

3.2. O gabinete do ATM deve possuir disjuntor elétrico de proteção geral corretamente dimensionado para o conjunto;

3.3. O conjunto formado pelo ATM e todos os seus componentes, inclusive o mini/microcomputador, deve requerer somente uma tomada, padrão ABNT NBR 14.136, para conexão à rede elétrica. Caso necessário, devem ser fornecidos adaptadores ou réguas de tomadas elétricas corretamente dimensionados para a soma das cargas do conjunto, sem prejuízo da vida útil do equipamento.

4. GABINETE

4.1. GABINETE SUPERIOR

4.1.1. Deve conter na parte frontal:

4.1.1.1. Monitor de vídeo,

4.1.1.2. Teclado vertical de função, nas laterais do monitor de vídeo;

4.1.1.3. Teclado numérico PIN PAD, abaixo do monitor de vídeo;

4.1.1.4. Saida de comprovantes impressos;

4.1.1.5. Leitor de cartão magnético;

4.1.1.6. Leitor de código de barras;

4.1.1.7. Dispensador de cédulas;

4.1.1.8. Espelhos de segurança;

4.1.1.9. Conector para fone de ouvido;

4.1.1.10. Câmera de segurança digital para identificação do usuário (cliente);

4.1.1.11. Câmera de segurança digital para monitoração do dispensador de cédulas;

4.1.1.12. Leitor biométrico de impressão digital.

4.1.2. O painel do operador deve estar situado na parte traseira do ATM;

4.1.3. Deve ser construído em chapa de aço SAE 1010/1020, equivalente ou superior, de, no mínimo, 3 milímetros de espessura, inclusive as portas;

4.1.4. A porta traseira poderá ser bipartida;

4.1.5. O fechamento da porta traseira deve ser feito por chave simples com segredo individual e travamentos em no mínimo dois pontos, com reforço em metal nos batentes;

4.1.6. O equipamento deve estar baseado em estrutura apropriada para instalação *in lobby*;

4.1.7. O acesso para suprimento deve ser exclusivamente pela parte traseira;

4.1.8. Os locais reservados para a fixação dos ícones de identificação visual do Banco deverão ser rebaixados e lisos, para permitir a melhor fixação desses.

4.2. GABINETE INFERIOR (COFRE)

4.2.1. O cofre deve ser construído com placas de aço SAE 1010/1020, equivalente ou superior, com propriedades antiperfurantes, antidesgaste e anticorte térmico, capazes de impedir perfuração mecânica e ataques com maçarico ou instrumentos similares de incisão de chama, utilizando composições metálicas e/ou multicamadas, que mantenham resistência contra ferramentas abrasivas, brocas, discos diamantados e calor extremo, preservando a integridade estrutural durante tentativas de violação, com espessura de, no mínimo, ½'' (meia polegada) em todas as faces, exceto a face inferior (piso) e na porta, que deverão possuir espessura total de 1'' (uma polegada) ou placas agregadas adicionais na placa anterior, que permitam resistência equivalente ou superior.

4.2.2. A soldagem das peças deve ser realizada com tecnologia *Metal Inert Gas* (MIG) ou superior. A paredes devem ser soldadas de forma contínua abrangendo as partes internas e externas;

4.2.3. Deve possuir proteção em "L" junto às dobradiças, fixadas na porta, estendida por toda a altura interna, de modo a impedir sua abertura em caso de violação dos ferrolhos ou dobradiça ou deve possuir, no mínimo 3 (três) ferrolhos na porta na lateral das dobradiças;

4.2.4. A parte traseira do cofre deve possuir dispositivo de fechamento eletrônico que atenda no mínimo aos seguintes requisitos:

4.2.4.1. Não deve conter senha de reset pelo teclado (restauração dos padrões de fábrica);

4.2.4.2. Possuir sistema de auto travamento ao fechar o mecanismo da porta;

4.2.4.3. Deve permitir programar as funções de retardo e abertura (janela) com variação de tempo de 0 minuto (default) a 99 minutos de retardo e 1 minuto (default) a 15 minutos (mínimo) de abertura (janela);

4.2.4.4. Possuir os usuários administrador (supervisor) e operador cadastrado de fábrica;

4.2.4.5. O usuário administrador/supervisor cadastrado de fábrica não deve possuir privilégios para realizar a abertura do cofre;

4.2.4.6. Deve ser acompanhado de manual de operação em português que traduza fielmente a programação do dispositivo de fechamento;

4.2.4.7. O mecanismo para definição e alteração dos segredos (senhas) deve funcionar sem a utilização de equipamentos especiais e/ou intervenção do fabricante.

4.2.5. Deve possuir dispositivo de auto travamento nas portas do cofre, que impeçam sua abertura quando da tentativa de violação do segredo da fechadura;

4.2.6. Deve possuir uma fechadura eletrônica com certificado UL tipo 1;

4.2.7. A região das fechaduras do cofre deve possuir proteção reforçada composta por caixa blindada antiperfurante, defletores anti-alavanca e proteção térmica contra maçarico e corte a plasma, impedindo ataques mecânicos, abrasivos ou térmicos que possam comprometer o mecanismo de abertura.

4.2.8. Deve possuir no mínimo 02 (dois) ferrolhos superiores;

4.2.9. Deve possuir no mínimo 02 (dois) ferrolhos inferiores;

4.2.10. Deve possuir no mínimo 03 (três) ferrolhos na lateral oposta às dobradiças;

4.2.11. Os ferrolhos deverão possuir diâmetro de, no mínimo, 1'' (uma polegada);

4.2.12. Os ferrolhos deverão ter penetração de travamento de, no mínimo, 3/4'' (três quartos de polegada);

4.2.13. Os ferrolhos deverão deslizar sobre a caixa da almofada e sobre um mancal interno, este em chapa de aço de, no mínimo, ½"'(meia polegada);

4.2.14. Os ferrolhos deverão ser dotados de sistema de *came*;

4.2.15. Os ferrolhos, bem como os mecanismos internos (came/eixo), deverão ser confeccionados em aço SAE 1010/1020, equivalente ou superior, cementado, temperado e revenido, com dureza superficial mínima de 50 HRC;

4.2.16. O cofre deve possuir saída lateral traseira para os cabos de alimentação elétrica e conectividade de rede local (LAN);

4.2.17. Deve possuir pés niveladores;

4.2.18. Deve possuir, no fundo do gabinete, sistema para permitir a fixação (chumbagem) no piso onde será instalado o equipamento, com no mínimo 5 (cinco) furos, sendo um na parte central/interna e quatro nas extremidades;

4.2.19. Deverão ser fornecidos 05 (cinco) *parabolts* para fixação, por equipamento; os *parabolts* devem ser de no mínimo, ½"'(meia polegada).

4.2.20. Deverá possuir 04 (quatro) rodas retráteis, compatíveis com o peso do ATM;

4.2.21. As rodas retráteis devem ser dotadas de mecanismo capaz de elevar o ATM a pelo menos 1cm (um centímetro) em relação ao piso. Esse mecanismo deverá ser acionando manualmente pelo interior do cofre;

4.2.22. Após a instalação do ATM as rodas devem ser embutidas de forma a permanecerem ocultas no interior do cofre;

4.2.23. As aberturas utilizadas pelas rodas devem ser protegidas para evitar a entrada de insetos e roedores no interior do ATM.

5. PAINEL DO OPERADOR

5.1. Deve estar localizado na parte traseira do gabinete superior;

5.2. Deve possuir monitor LCD com Touch Screen;

5.3. Deve possuir leitor de cartão magnético (trilha 2);

5.4. O acesso aos componentes do painel do operador deve ocorrer sem que haja a necessidade de abertura do gabinete superior.

6. MONITOR DE VÍDEO

6.1. O ATM deve possuir monitor de vídeo do tipo *Light Emitting Diode* (LED) , tela plana, de no mínimo 15” (quinze polegadas) na diagonal, com matriz ativa e tratamento antirreflexo e antiestático;

6.2. O monitor deve ser do tipo Touch Screen;

6.3. O monitor deve ter sido projetado para uso em ATM, não sendo aceitas adaptações que utilize monitor de vídeo com gabinete/moldura saliente nas bordas frontais da tela;

6.4. A tela deve possuir transparência igual ou superior a 90%;

6.5. A tela deve ser resistente a risco, a poeira, a gordura e a ataques químicos, de forma a manter a integridade do material;

6.6. O monitor deve ser fixado de modo seguro, dificultando quaisquer tentativas de violação, deve manter perfeito alinhamento com o painel do terminal, sem a presença de frestas que possam permitir a inserção de objetos estranhos;

6.7. A resolução nativa deve ser de, no mínimo, 1.920 (um mil novecentos e vinte) pontos na horizontal e 1.080 (um mil e oitenta) pontos na vertical ou superior (Full HD);

6.8. Deve possuir taxa mínima de atualização de 60Hz a 75Hz;

6.9. Deve possuir tempo de resposta entre 4ms e 6ms;

6.10. Deve possuir taxa de brilho de no mínimo 250cd/m2 (duzentas e cinquenta candelas por metro quadrado);

6.11. A tela do monitor de vídeo deve possuir revestimento antirreflexo;

6.12. Devem suportar no mínimo 16 Milhões de cores;

6.13. Devem possuir contraste estático ou dinâmico, no mínimo de 5.000.000:1;

6.14. Deve possuir controles para regulagem das configurações de exibição, tais como cor, brilho, contraste, gama, posição da imagem, reset de fábrica, autoajuste. Esses controles de ajustes não devem estar disponíveis para os usuários;

6.15. Deve possuir certificação Energy Star 5.0 ou superior;

6.16. Deve possuir proteção contra vandalismo;

6.17. Deve possuir ângulo de visão mínimo de 110º na horizontal e de 110º na vertical;

6.18. Deve contar com filtro de tela que mantenha a privacidade do usuário, em visualização horizontal;

6.19. Deve possuir ângulo de visão vertical que permita a visibilidade das informações na tela por usuários nas condições definidas abaixo:

6.19.1. Usuário em pé, com estatura entre 1,45 m e 1,95;

6.19.2. Usuário em cadeiras de rodas, com altura de visão de 1,15 m (altura dos olhos do usuário em relação ao piso de referência) conforme determina a Norma ABNT NBR 15250:2005.

7. MICROCOMPUTADOR INTEGRADO

7.1. SOFTWARE BÁSICO, SISTEMAS E APLICATIVOS

7.1.1. Os microcomputadores devem estar devidamente licenciados junto a Microsoft para utilização do sistema operacional Microsoft Windows 11 Professional 64bits, no idioma português brasileiro;

7.1.2. Devem ser disponibilizados drivers compatíveis com o sistema operacional Microsoft Windows 11 Professional/Enterprise 64bits para os componentes do Desktop; os drivers devem ser disponibilizados em mídia USB e/ou a partir de sítio na internet;

7.1.3. Após a assinatura do contrato o CONTRATANTE realizará a instalação e configuração do sistema operacional, softwares básicos e aplicativos no equipamento apresentado como amostra pelo CONTRATADO;

7.1.4. A partir do equipamento configurado o CONTRATANTE construirá a imagem do sistema operacional, softwares básicos e demais aplicativos e encaminhará a imagem ao CONTRATADO, que por sua vez deve aplicar essa imagem ao seu processo fabril, de forma que o CONTRATANTE receba todos os ATM devidamente configurados com a imagem construída pelo Banco;

7.1.5. O CONTRATADO deve garantir a aplicação da imagem construída pelo CONTRATANTE assegurando que o seu processo fabril é livre de erros, falhas e conflitos e que defina automaticamente um *Security Identifier* (SID) do sistema operacional Microsoft Windows 11 exclusivo para cada unidade submetida ao processo de baixa de imagem;

7.1.6. O CONTRATANTE poderá, ao seu critério, exigir a participação presencial ou remota de técnico do CONTRATADO para apoiar na construção da imagem, que será construída nas dependências do CONTRATANTE;

7.1.7. Devem ser disponibilizadas ao CONTRATANTE mídias Universal Serial Bus (USB) contendo a imagem final do sistema operacional, softwares básicos e aplicativos para uso em casos de recuperação de falhas e novas baixas de imagem;

7.1.8. O CONTRATADO deve manter processo documentado de cópias de segurança das imagens, configurações, certificados e parâmetros operacionais do ATM, incluindo testes periódicos de restauração em alinhamento com os RTO e RPO definidos pelo CONTRATANTE. Evidências dos testes devem ser fornecidas sempre que solicitadas.

7.1.9. O sistema operacional e os softwares básicos devem seguir baseline de segurança baseada em CIS Benchmarks ou equivalente, incluindo: controle de execução de binários assinados, desativação de protocolos legados (SMBv1, NTLMv1 e TLS < 1.2), restrição lógica e física ao uso de portas USB, hardening de serviços, políticas de auditoria estendida e coleta de logs avançados. Alterações não autorizadas na configuração de segurança devem ser impedidas pelo ambiente.

7.1.10. O CONTRATADO deve fornecer no mínimo 40% (quarenta por cento) de mídias de imagem do sistema operacional, softwares básicos e aplicativos, tomando como base o quantitativo de ATM objeto deste Edital.

7.2. GABINETE

7.2.1. O gabinete dever ser do tipo Mini PC ou uATX (micro ATX);

7.2.2. Deve ser armazenado internamente ao cofre do ATM.

7.3. ALIMENTAÇÃO ELÉTRICA

7.3.1. A fonte de alimentação deve estar corretamente dimensionada para suportar a carga exigida pelo conjunto;

7.3.2. A alimentação elétrica deve ser integrada ao ATM;

7.3.3. Deve possuir a certificação 80 Plus na categoria Gold ou superior;

7.3.4. Deve possuir *Power Factor Correction* (PFC) ativo.

7.4. PLACA MÃE

7.4.1. Deve implementar a utilização de *Input/Output System* (BIOS) ou *Unified Extensible Firmware Interface* (UEFI), com a possibilidade da utilização de senha para acesso às configurações do microcomputador;

7.4.2. O BIOS ou UEFI devem disponibilizar informações referentes ao número de série e modelo do ATM, através de acesso via software, a partir do sistema operacional. Não será necessário fornecer softwares adicionais para extrair informações do BIOS ou UEFI;

7.4.3. O BIOS ou UEFI deve possuir as informações do fabricante, modelo e número de série do equipamento (ATM) permitindo leitura remota via *Windows Management Instrumentation Command Line* (WMIC), sendo possível recuperar as informações a partir dos seguintes comandos:

7.4.3.1. **wmic computersystem get manufacturer**;

7.4.3.2. **wmic computersystem get model**;

7.4.3.3. **wmic systemenclosure get serialnumber**.

7.4.4. As informações sobre o fabricante, modelo e número de série do equipamento (ATM) devem ser mantidas em caso de substituição da placa mãe; caso necessário deve ser fornecido utilitário para gravação destas informações no BIOS ou UEFI;

7.4.5. O ATM deve possuir a capacidade de monitoramento do hardware incluindo: temperatura do sistema, temperatura do processador, voltagem etc.;

7.4.6. O BIOS ou UEFI devem ser compatíveis com os modos de economia de energia do sistema operacional Microsoft Windows 11 ou superior, otimizando o consumo de energia de dispositivos como placa principal, disco rígido e monitor de vídeo;

7.4.7. O BIOS ou UEFI deve ser desenvolvida de acordo com o padrão de segurança NIST 800 147 ou ISO/IEC 19678:2015;

7.4.8. O ATM deve possuir Secure Boot ativado e configurado de fábrica, impedindo a inicialização de qualquer firmware, driver ou carregador de boot não assinado digitalmente pelo fabricante ou pelo CONTRATANTE. A solução deve permitir auditoria remota do estado do Secure Boot, registrando tentativas de desativação.

7.4.9. Todos os firmwares dos módulos críticos (BIOS/UEFI, EPP, leitor biométrico, módulo pagador, sensores e demais periféricos) devem ser assinados digitalmente. O ATM não deve aceitar firmwares sem assinatura válida ou com assinatura revogada.

7.4.10. O microcomputador deve possuir ferramenta que possibilite realizar a formatação definitiva dos dispositivos de armazenamento, desenvolvida em acordo com o padrão de segurança NIST 800- 88 ou ISO/IEC 27040:2024. Caso esta ferramenta não seja nativa da BIOS ou UEFI, deve ser oficialmente homologada pelo FABRICANTE do ATM;

7.4.11. Atualizações Seguras de Firmware e Software O CONTRATADO deve implementar processo seguro de distribuição, validação e instalação de atualizações de firmware, BIOS/UEFI, drivers e módulos embarcados. Toda atualização deve ser entregue por canal autenticado, assinada digitalmente e verificada pelo ATM antes da aplicação. O equipamento deve impedir downgrade não autorizado (rollback protection) e registrar, em log assinado, todas as tentativas de atualização, bem□sucedidas ou não. O CONTRATADO deve apresentar política formal de ciclo de vida de firmware, contendo prazos máximos de correção para vulnerabilidades críticas.

7.4.12. Deve possuir chip de segurança *Trusted Platform Module* (TPM) soldado à placa mãe ou *Firmware Trusted Platform Module* (fTMP A tecnologia TPM ou fTMP fornecida deve ser no mínimo da versão 2.0. Devem ser fornecidos todos os drivers necessários à sua utilização;

7.4.13. O TPM ou fTPM deve ser completamente compatível com o Microsoft Windows 11 e Linux Ubuntu e derivados;

7.4.14. Deve permitir a inicialização do sistema operacional a partir de dispositivos de interface SATA, NVMe e USB.

7.5. **PROCESSADOR**

7.5.1. A geração do processador deve ser a penúltima ou última geração lançada pelo fabricante do processador;

7.5.2. Caso o processador seja Intel, deve ser no mínimo da família Core I5; caso seja AMD deve ser no mínimo da família Ryzen 5 PRO;

7.5.3. O processador deve possuir no mínimo 06 (seis) núcleos/cores, sem considerar tecnologias de *Multi-Threading*, *Hyper-Threading* ou tecnologias semelhantes;

7.5.4. O processador deve possuir tecnologia *Multi-Threading*, *Hyper-Threading* ou tecnologias semelhantes;

7.5.5. Deve suportar a execução de instruções em 64bits e 32bits;

7.5.6. Deve ter sido produzido para utilização em microcomputador Desktop; não serão aceitos processadores desenvolvidos para a linha Mobile;

7.5.7. Deve suportar a comunicação com os bancos de memória em modo *Dual Channel*;

7.5.8. Deve ser compatível com memórias do tipo DDR 5 ou superior.

7.6. **MEMÓRIA RAM**

7.6.1. O ATM deve possuir no mínimo 16GB (dezesseis Gigabytes) de memória RAM;

7.6.2. A memória RAM total deve estar disposta e configurada em modo *Dual Channel*;

7.6.3. A memória deve ser no mínimo do tipo DDR 5, devendo possuir a frequência de operação máxima admitida pelo processador e placa mãe.

7.7. **CONTROLADORA DE VÍDEO**

7.7.1. Caso seja integrada ao processador deve possibilitar o compartilhamento de no mínimo 2GB (dois gigabytes) da memória principal do sistema; caso seja dedicada deve possuir no mínimo 2GB (dois gigabytes) de memória RAM ou superior;

7.7.2. Deve possuir acelerador gráfico integrado, com características técnicas e desempenhos iguais ou superiores aos adaptadores Intel Iris Graphics ou Intel UHD Graphics ou AMD Radeon Graphics;

7.7.3. Deve suportar resolução de vídeo no mínimo Full HD;

7.7.4. A frequência da *Graphics Processing Uni*t (GPU) deve ser de 1550Mhz (Mil quinhentos e cinquenta mega-hertz) ou superior;

7.7.5. Deve ser compatível com Microsoft DirectX e *Windows Display Driver Model* (WDDM).

7.8. **SUBSISTEMA DE ARMAZENAMENTO**

7.8.1. Não serão aceitas unidades de armazenamento mecânicas;

7.8.2. Deve possuir 01 (uma) unidade de armazenamento interna com capacidade mínima de 480GB (quatrocentos e oitenta gigabytes);

7.8.3. A unidade de armazenamento deve ser do tipo PCIe NVMe M.2 ou tecnologia superior;

7.8.4. Unidades de armazenamento que precisem ser substituídas, por motivos de manutenção preventiva e/ou corretiva, permanecerão em posse do CONTRATANTE, por medida de segurança e confidencialidade das informações ali armazenadas;

7.8.5. A unidade de armazenamento deve estar protegida por criptografia integral de disco (Full Disk Encryption), utilizando BitLocker, LUKS ou solução equivalente, com as chaves protegidas pelo TPM 2.0 ou fTPM. A descriptografia deve ocorrer apenas após validação de integridade do boot.

7.8.6. A unidade de armazenamento deve possuir tecnologia *Self-Monitoring Analysis and Reporting Technology* (*SMART*);

7.8.7. A unidade de armazenamento deve possuir *Mean Time Between Failures*/Tempo Médio entre Falhas (MTBF) de no mínimo 1.500.000h (um milhão e quinhentas mil horas).

7.9. INTERFACES DE CONEXÃO

7.9.1. Após a conexão de todos os periféricos e sensores, o microcomputador deve disponibilizar no mínimo 02 (duas) portas USB livres;

7.9.2. Será aceita a utilização de hubs/adaptadores para expansão da quantidade de portas USB do microcomputador, desde que estejam acomodados dentro do gabinete superior ou do cofre;

7.9.3. Deve possuir portas suficientes para a conexão de todos os periféricos e componentes do equipamento, sejam eles conectados por interfaces USB ou seriais RS 232;

7.9.4. Deve disponibilizar interface de conexão USB, de fácil acesso, para os serviços de implantações, manutenções e demais intervenções. A interface deve estar disponível apenas caso a porta do gabinete superior ou do cofre estejam abertas.

7.10. ADAPTADOR DE REDE LOCAL

7.10.1. Deve possuir interface RJ-45 padrão Ethernet;

7.10.2. Deve suportar o padrão Gigabit Ethernet;

7.10.3. Deve permitir operação em modo *full-duplex* nas velocidades 10/100/1000Mbps, *auto-sensing*;

7.10.4. Deve possuir as tecnologias *Wake-up on LAN* (WOL) e *Preboot Execution Environment* (PXE) permitindo ligar a CPU remotamente através do adaptador de rede.

7.10.5. Toda comunicação entre o ATM e os sistemas centrais do CONTRATANTE deve utilizar protocolo seguro TLS 1.2 ou superior, preferencialmente TLS 1.3, com autenticação mútua baseada em certificados digitais emitidos por Autoridade

Certificadora confiável pelo CONTRATANTE. É vedada a utilização de conexões em texto claro.

7.10.6. Além do uso obrigatório de TLS 1.2 ou superior, o ATM deve implementar exclusivamente cipher suites modernas, desativando algoritmos depreciados. É obrigatório o uso de autenticação mútua (mTLS) para comunicação com sistemas centrais. Os certificados utilizados devem possuir rotação periódica automática, e suas chaves privadas devem ser armazenadas e protegidas exclusivamente pelo TPM 2.0 ou fTPM.

7.10.7. O CONTRATADO deve assegurar a gestão completa do ciclo de vida dos certificados digitais utilizados no ATM, incluindo emissão, distribuição segura, armazenamento protegido, rotação periódica, revogação, expiração e monitoramento contínuo. A solução deve rejeitar automaticamente certificados inválidos ou revogados.

7.11. **ÁUDIO**

7.11.1. A controladora de áudio deve permitir a reprodução de som em alta definição (*High Definition*) com resolução mínima de 16 (dezesseis) bits;

7.11.2. Os microcomputadores devem possuir autofalante interno (*Buzzer*) que permita a emissão de sons de alerta (*Beep*) sobre o funcionamento e falhas do equipamento;

7.11.3. deve possuir conexão para fones de ouvido e microfone conforme determina a Norma ABNT NBR 15250:2005;

7.11.4. A interface para conexão do fone de ouvido deve estar disponível aos usuários no painel frontal do ATM;

7.11.5. Serão aceitos microcomputadores que compartilhem uma única conexão frontal de áudio para fone de ouvido e microfone.

8. IMPRESSORA DE RECIBOS

8.1. A impressora deve ser térmica, com guilhotina e *presenter*;

8.2. A impressora deve imprimir no mínimo 48 caracteres por linha, em modo normal;

8.3. A impressora deve possuir no mínimo sensores que indiquem:

8.3.1. pouco papel;

8.3.2. término do papel; e

8.3.3. papel enganchado (enrosco).

8.4. Deve possuir velocidade de impressão de no mínimo 10 linhas por segundo (LPS);

8.5. Deve ser capaz de imprimir caracteres maiúsculos, minúsculos e especiais, com todos os caracteres da língua portuguesa, suportando os conjuntos de caracteres ASCII e/ou ABICOMP e code page 850 e 437;

8.6. Deve possuir Buffer de no mínimo 10 KB (dez quilobytes);

8.7. Deve possuir guilhotina e *presenter* controláveis por software, com método de corte do papel do tipo *scissor cut*;

8.8. Deve possuir sistema de proteção do *presenter* controlável por software contra obstrução e retirada brusca de recibo;

8.9. Deve suportar bobina de, no mínimo, 76 mm (setenta e seis milímetros) de largura e 9” (nove polegadas) de diâmetro externo;

8.10. O módulo impressor deve estar perfeitamente alinhado com o bocal do painel frontal, evitando desvios ou enroscos na saída do papel;

8.11. O módulo impressor deve ser instalado em sistema de trilhos deslizantes para facilitar a manutenção e o acesso aos locais de provável enrosco de papel (módulo de impressão e bocal) e troca de consumível;

8.12. A impressora deve ser capaz de imprimir figuras;

8.13. A impressora deve suportar a impressão em modo gráfico, inclusive código de barras e QRCode;

8.14. Deverão ser fornecidas 02 (duas) bobinas de papel, compatível com a impressora, por equipamento.

9. LEITOR DE CARTÕES

9.1. Deve ser de inserção manual (DIP), híbrido, capaz de ler tarja magnética e Chip EMV (*Smart Card*);

9.2. O leitor de cartões deve ter capacidade de leitura das trilhas 1, 2 e 3, simultaneamente, nos padrões ABA/ISO;

9.3. Deve ter capacidade de leitura e gravação de *Smart Card* com as seguintes características:

9.3.1. Aderência aos padrões ISO 7816/1-3 e EMV Versão 4.x;

9.3.2. Suporte aos protocolos T=0 e T=1;

9.3.3. Reconhecer *Smart Card* pertencente às classes “A”, “B”, “AB” e “C”.

9.4. Deve possuir certificado de aprovação EMV versão 4.x; deve ser apresentada cópia junto com a documentação técnica, não sendo aceita a reprodução de páginas da Internet;

9.5. Possuir sensores de detecção de presença de cartão selado (com chip) e de identificação de tarja magnética;

9.6. Deve ser dotado de dispositivo para retenção do cartão, durante a operação com *Smart Card;*

9.7. Deve possuir compatibilidade com a interface PC/SC (*Personal Computer/Smart Card*);

9.8. Possuir criptografia de hardware para impedir a violação da comunicação do módulo e do ATM;

9.9. Possuir sistema *Antiskimming* com proteção para a leitora de cartões, para detectar tentativas de fraude.

9.10. O leitor de cartões deve possuir mecanismos de detecção e resposta contra ataques do tipo *Shimming*, capazes de interceptar comunicações entre o chip EMV e o módulo leitor.

10. LEITOR DE CÓDIGO DE BARRAS

10.1. Deve permitir leitura óptica e decodificação de códigos de barras padrão FEBRABAN, 2/5 intercalado (ANSI MH 10.8M – 1983) e código 39 (MIL-STD 1189, ANSI MH 10.8M – 1983);

10.2. Deve apresentar índice máximo de rejeição de documentos de 4% (quatro por cento);

10.3. Deve ser capaz de ler documentos de cobrança, conforme padrão adotado pela Federação Brasileira de Bancos (FEBRABAN), em estado normal de utilização, considerando papéis manipulados, com dobras ou amassados, de espessura e gramatura diferentes;

10.4. Deve realizar a leitura ótica e decodificação de padrão 2D (QrCode) padrões PDF417, Data Matrix, QR Code, considerando papéis manipulados, com dobras ou amassados, de espessura e gramatura diferentes e telas de dispositivos móveis, como smartphones, tablets e outros dispositivos pessoais móveis;

10.5. O leitor deve funcionar corretamente em salas com diferentes tipos de iluminação natural e artificial, incluindo as iluminações de LED.

11. LEITOR BIOMÉTRICO

11.1. Deve ser baseado na tecnologia de identificação dos padrões biométricos da impressão digital (*Finger Print)*;

11.2. O dispositivo biométrico deve possuir solução de *tamper proof* a fim de proteger as chaves criptográficas armazenadas no sensor biométrico e a placa de circuito impresso responsável pela captura e manipulação de *templates*;

11.3. Deve utilizar sistema multiespectral para captura/leitura dos dados;

11.4. O dispositivo deve capturar imagens precisas e de alta qualidade da superfície e subsuperfície da impressão digital, simultaneamente;

11.5. O dispositivo deve possuir bateria interna, para preservação da chave criptográfica, com tempo de vida útil estimado em no mínimo 05 (cinco) anos;

11.6. Deverá utilizar Interface USB 2.0 ou superior;

11.7. O formato de armazenamento do perfil biométrico deverá atender às normas ISO 19794-2 – *Biometric data interchange formats*;

11.8. O Algoritmo de *Match* deverá possuir a certificação MINEX III do NIST, para o extrator e para o *matcher*, comprovada por declaração apresentada pelo fabricante do algoritmo e por consulta ao site http://www.nist.gov;

11.9. Os dispositivos destinados ao registro e à autenticação deverão possuir a mesma qualidade (não será utilizada a captura rolada de impressão digital na fase do registro do usuário);

11.10. Deve ser permitida a calibragem do dispositivo para o estabelecimento do limiar *default* de comparação, via API ou no ato da comparação por meio de envio do limiar como parâmetro, para tanto, os comandos deverão ser criptografados e assinados;

11.11. O dispositivo biométrico deve ser dotado de funções como *live-finger detection*, *anti-spoofing*, *latente rejection* e ser capaz de resistir a fraudes como:

11.11.1. Imagens impressas que repliquem impressões digitais;

11.11.2. Impressões digitais simuladas com materiais como silicone ou gelatina;

11.11.3. Dedos reais amputados;

11.11.4. Dedos falsos com imitação de digitais.

11.12. O dispositivo biométrico não poderá ser fixado apenas na chapa de aço, devendo também existir solução interna complementar de fixação;

11.13. Deve ser resistente a pequenas descargas eletrostáticas, que podem ocorrer quando o usuário tocar o dispositivo;

11.14. Deve manter as funcionalidades, sem perda significativa de performance, mesmo diante de condições inadequadas, como diferentes níveis de luminosidade ambiente, poeira, umidade, suor, camadas finas de óleos, cremes e gorduras eventualmente portadas pelos usuários;

11.15. Deverá ser robusto e resistente a choques, arranhões e desgastes superficiais, considerando condições de uso superiores a 05 (cinco) anos, inclusive quanto à garantia de manutenção e reposição de peças;

11.16. Todos os módulos de software, incluindo drivers, deverão ter seus códigos fonte, bem como a documentação e scripts de compilação, entregues e ter a permissão de uso ilimitada cedida ao CONTRATANTE;

11.17. Deverá conter proteção lógica e física contra atualizações de *firmware* garantindo a integridade do conteúdo dele;

11.18. O tamanho do perfil biométrico gerado para armazenamento não deverá ultrapassar 900 bytes;

11.19. O dispositivo biométrico deverá conter número único de identificação e deve ser capaz de:

11.19.1. Operar com os algoritmos de criptografia RSA com chaves de tamanho mínimo de 2048 bits e AES com chave mínima de 256 bits;

11.19.2. Operar com algoritmos de *hash* SHA-256 ou superior;

11.19.3. Gerar desafio e conferir resposta (número aleatório/criptogramas);

11.19.4. Deve ser capaz de processar a comparação no próprio dispositivo, recebendo da aplicação o perfil biométrico criptografado e o limiar de comparação – FMR e processando a comparação;

11.19.5. Deve ser permitida a calibragem do dispositivo para o estabelecimento do limiar *default* de comparação, via API através de comandos criptografados e/ou assinados;

11.19.6. O dispositivo biométrico deverá apresentar precisão de pelo menos 0,1% tanto para FAR quanto para FRR no modo de funcionamento EER (condições de teste com usuários reais);

11.19.7. Deverá ser resistente à abertura e intrusão (FIPS ou TRMS) e ser lacrado com mecanismo interno de autodestruição em caso de violação (*Tamper Proof*);

12. TECLADO ENCRYPTING PIN PAD

12.1. O Teclado *Encrypting* PIN PAD (EPP) deve ser do tipo mecânico;

12.2. As teclas devem ser em aço inoxidável e possuir proteção contra vandalismo, uso intenso e condições climáticas adversas, inclusive em ambientes externos;

12.3. Deve ser blindado, com detecção de invasão e destruição das chaves em caso de violação (*tamper proof*);

12.4. Deve possuir apenas 01 (um) teclado (EPP);

12.5. Não será aceito teclado de membrana;

12.6. As teclas não podem possuir cantos vivos;

12.7. Deve possuir no mínimo 16 (dezesseis) teclas;

12.8. Deve ser capaz de operar com os algoritmos de criptografia RSA e 3-DES com chaves de tamanho mínimo de 2048 bits para RSA e 168 bits para 3-DES;

12.9. Deve suportar o padrão X509 para certificados;

12.10. Deve possuir compatibilidade com funções de *Hash* baseadas em algoritmos SHA-2;

12.11. Deve ser capaz de gerar e armazenar pares de chaves RSA de no mínimo 2048 bits;

12.12. Ser capaz de armazenar, no mínimo, 04 (quatro) chaves de trabalho 3-DES *Double Length*;

12.13. Deve ser capaz de gerar desafio e conferir resposta (número aleatório/criptograma 3-DES);

12.14. Deve dispor de mecanismos para troca e carregamento local e remoto das chaves;

12.15. Deve ser homologado de acordo com a norma PCI EPP em sua versão atualizada em laboratório indicado pela VISA;

12.16. Deve conter número único de identificação;

12.17. O teclado deve permitir a inserção de *Master Key* para encriptação de dados das seguintes maneiras:

12.17.1. Custodiado, ou seja, em fábrica com utilização de *Hardware Security Module* (HSM) evitando assim a inserção manual das chaves;

12.17.2. Em produção, por meio de software mediante acesso local e remoto;

12.17.3. A solução de criptografia oferecida deve permitir a inserção, remoção e troca da chave através de processo remoto, via rede, com uso de chave cadastrada para esse processo ou por uma das chaves já inseridas. Deve ser fornecida, sem ônus adicionais, as APIs e documentação necessária para que o Banco possa adequar seu sistema para esta tarefa.

12.17.4. O processo de gestão de chaves criptográficas deve prever rotação periódica obrigatória, segregação de funções entre operadores e trilha de auditoria completa das operações de geração, inserção, substituição e descarte de chaves. A solução deve registrar logs assinados digitalmente para todas as operações de chaveamento.

12.17.5. A solução deve implementar política de governança de chaves, incluindo rotação periódica obrigatória, segregação de funções entre operadores e trilhas de auditoria assinadas criptograficamente para todas as operações envolvendo chaves.

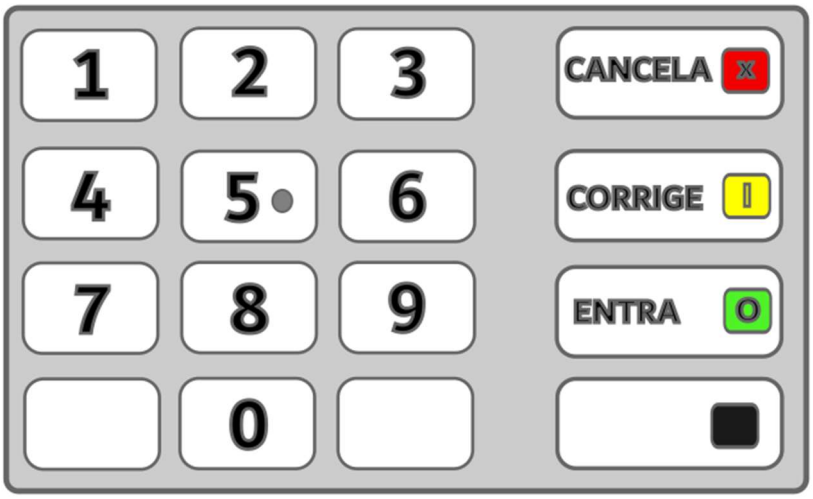
12.18. O teclado deve ser personalizado no momento da fabricação com o par de chaves RSA e certificado X509v3 assinado por autoridade certificadora confiável. O(s) certificado(s) da autoridade certificadora utilizada para assinatura dos certificados dos EPP deve(ão) ser entregue(s) ao CONTRATANTE;

12.19. Deve ser entregue certificação que comprove o atendimento às exigências de segurança estabelecidas pela Visa e Mastercard Internacionais para transações de débito e crédito, junto com a documentação técnica;

12.20. O teclado deve obedecer ao que preconiza a Norma ABNT NBR 15250:2005, quanto as cores e marcações em alto relevo das teclas ENTRA, CORRIGE, CANCELA e a tecla correspondente ao número 5, conforme tabela a abaixo:

TECLA	COR	MARCAÇÃO
CANCELA	Vermelha	**X**
CORRIGE	Amarela	**I**
ENTRA	Verde	**O**
5	**---**	●

12.21. O teclado deve observar o seguinte *layout*:



12.22. O teclado deve possuir as seguintes teclas:

12.22.1. Números de 0 a 9;

12.22.2. Tecla CANCELA ou ANULA;
12.22.3. Tecla CORRIGE;

12.22.4. Tecla ENTRA;

12.22.5. No mínimo 03 (três) teclas de expansão.

13. TECLADO VERTICAL DE FUNÇÕES

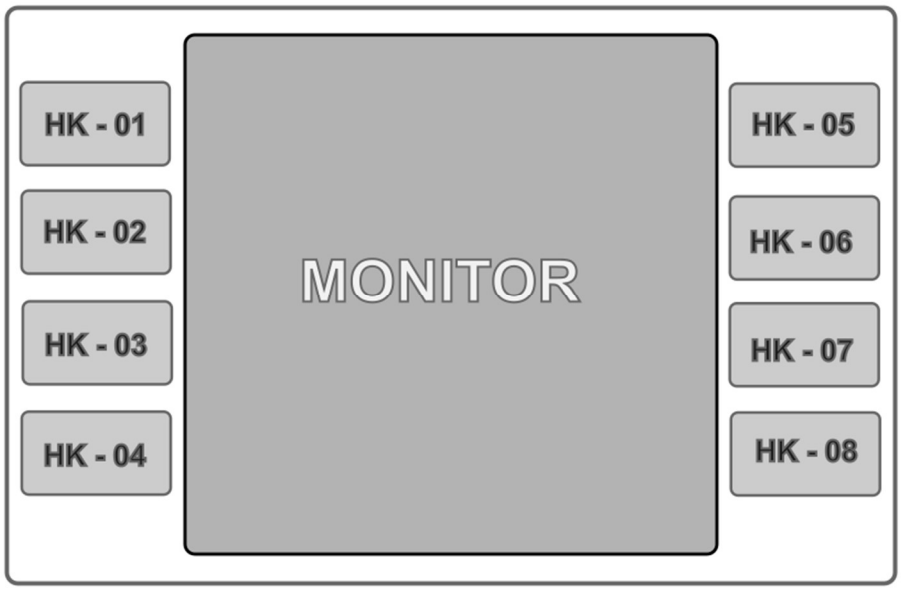
13.1. O teclado deve ser mecânico;

13.2. As teclas devem ser em aço inoxidável ou plásticos industriais de alta densidade e possuir proteção contra vandalismo, uso intenso e condições climáticas adversas, inclusive em ambientes externos;

13.3. Deve possuir 08 (oito) teclas divididas em dois grupos, à direita e à esquerda do monitor de vídeo; as teclas não devem possuir texto ou marcação;

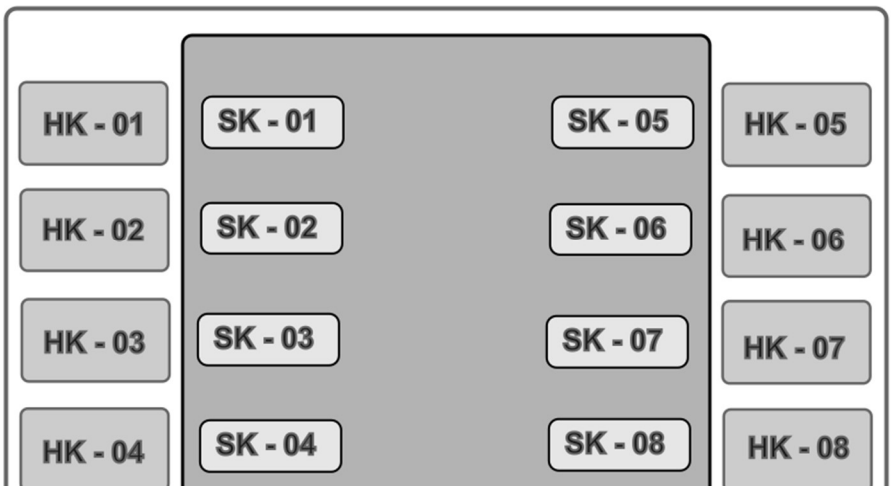
13.4. As teclas deverão ser programáveis para retornar qualquer um caractere do código ASCII:

13.5. O *layout* das teclas físicas (HK) deve seguir, conforme mostrado na figura abaixo:



13.6. As dimensões das teclas devem obedecer a Norma ABNT NBR 15250:2005;

13.7. Deve haver alinhamento entre as teclas físicas (HK) do teclado vertical de funções com as teclas virtuais (SK) apresentadas pelo aplicativo do Banco; o alinhamento pode consistir no posicionamento das teclas reais ou na utilização de guias que façam a ligação visual entre a tecla real e a tecla virtual, conforme exemplificado no exemplo a seguir:



14. CONECTOR PARA FONES DE OUVIDO

14.1. O gabinete superior deve possuir conector para fone de ouvido no padrão P2 (*mini-Jack*), com volume do som controlado através de botões individuais de pressão ou toque, permitindo que se aumente ou abaixe o volume imediatamente após o seu acionamento;

14.2. O conector deve ser instalado rente ao painel, e ter sua superfície circunvizinha côncava, de forma a orientar o curso de inserção do plugue.

15. CÂMERA DE VÍDEO PARA MONITORAÇÃO DO USUÁRIO (CLIENTE)

15.1. O painel superior deve possuir câmera de vídeo digital, com resolução de, no mínimo, 2 MP, com no mínimo 16 bits de cores;

15.2. A câmera deve possuir campo visual de mínimo de 60° (sessenta graus);

15.3. Deve permitir fotografar nitidamente em ambientes com diferentes graus de luminosidade direta no equipamento, com iluminância a partir de 0,1 lux;

15.4. Deve fotografar o rosto de usuários posicionados à frente do terminal (considerando a largura do equipamento), tanto em pé, com estatura, no mínimo, entre 1,45 m e 1,95 m, quanto em cadeira de rodas, com altura de visão (altura dos olhos do usuário em relação ao piso de referência) de, no mínimo, 1,15 m, sem focalizar o teclado PIN;

15.5. A câmera deve estar protegida por vidro, espelho ou acrílico de alta resistência que impeça o acesso direto ao dispositivo através do painel frontal, sem prejuízo à qualidade da imagem.

16. CÂMERA DE VÍDEO PARA MONITORAÇÃO DO MÓDULO PAGADOR

16.1. O ATM deve possuir câmera direcionada ao compartimento de saque e depósito (pocket) e iluminação para permitir que as operações de saque e depósito sejam monitoradas;

16.2. Deve ser digital, com resolução de, no mínimo, 2 MP, com no mínimo 16 bits de cores;

16.3. Deve permitir fotografar e filmar nitidamente em ambientes com diferentes graus de luminosidade direta no equipamento, com iluminância a partir de 0,1 lux;

16.4. Deve gravar em formato de vídeo ou GIF, com a quantidade de frames que permita a visualização da ação;

16.5. Deve possuir LED interno, próximo à câmera, de forma a permitir a iluminação adequada para a gravação.

17. MÓDULO PARA DEPÓSITO E PAGAMENTO DE CÉDULAS

17.1. Deve possuir acesso frontal;

17.2. Deve ser capaz de realizar pagamento (reciclagem) a partir das cédulas depositadas;

17.3. Deve possuir *presenter* com *shutter*;

17.4. Todos os cassetes devem ser identificados;

17.5. Deve implementar a funcionalidade de detecção de cédulas por meio de teste de espessura;

17.6. A entrega de cédulas deve ser realizada por meio de *presenter*;

17.7. Deve ser capaz de pagar, no mínimo, 30 (trinta) cédulas;

17.8. Deve ser capaz de realizar o recolhimento integral do maço de cédulas não retirado após o tempo parametrizado;

17.9. A quantidade de cédulas por pagamento deve ser programável por aplicativo;

17.10. Deve manusear cédulas novas e usadas;

17.11. Deve manusear cédulas de papel moeda e polímero;

17.12. Deve possuir, no mínimo, 04 (quatro) cassetes para cédulas;

17.13. Os cassetes deverão ser auto-lacrantes e lacráveis;

17.14. Cada cassete deve acomodar, no mínimo, 2.500 (duas mil e quinhentas) cédulas novas;

17.15. Deve ser compatível com as cédulas da primeira e da segunda família emitidas pela Casa da Moeda do Brasil em circulação e/ou divulgadas pelo Banco Central do Brasil (BACEN), sendo permitidos ajustes (regulagens, instalações ou desinstalações de peças), desde que simplificados e sem a necessidade de mudanças em outros componentes do módulo pagador ou do Terminal de Autoatendimento;

17.16. Deve possuir, no mínimo, 01 (um) cassete para cédulas rejeitadas;

17.17. O cassete para cédulas rejeitadas deve comportar no mínimo 150 (cento e cinquenta) cédulas;

17.18. O cassete de cédulas rejeitadas deve estar localizado em área segura ou possuir dispositivo de segurança antifurto que impeça qualquer acesso pelo bocal de saída das cédulas;

17.19. O módulo deve ser dotado de dispositivo de proteção de hardware ou de software contra a fraude na modalidade “Retenção de Cédulas” (plaqueta afixada com adesivo ou elemento colante, instalado no bocal da saída das cédulas que impede o recolhimento delas) e suas variantes, como a inserção de objetos estranhos no bocal do módulo;

17.20. O módulo deve realizar a rejeição de cédulas duplas e fora de especificação de forma individual (uma a uma);

17.21. A área de transporte das cédulas deve estar protegida por tampa em material resistente, que impeça violações por esta entrada;

17.22. A rejeição deve operar de forma individual (uma a uma) para cédulas duplas e fora de especificação;

17.23. O módulo deve estar perfeitamente alinhado com o bocal do painel frontal, evitando desvios ou enrosco na saída de cédulas;

17.24. O módulo deve ser instalado em sistema de trilhos deslizantes para facilitar a manutenção e o acesso aos locais de provável enrosco de cédulas, compatível com o peso e dimensões do módulo pagador e dos cassetes com sua capacidade plena, inclusive quando movimentados para fora do cofre; deve possuir sistema de travamento que impeça o deslocamento involuntário dos cassetes durante a movimentação do módulo; deve ser dotado de puxador localizado em posição funcional e ergonômica;

17.25. O módulo deve permitir a inserção de Master Key (3DES ou AES) para encriptação de dados em modo custodiado, ou seja, por inserção realizada em fábrica com utilização de *Hardware Security Module* (HSM) evitando assim a inserção manual das chaves;

17.26. Os módulos devem sair de fábrica com uma chave única (versão 0), que funcionará como uma chave de transporte, que não possibilite comandos de dispensa. Esta chave deve ser substituída assim que o equipamento entrar em funcionamento e devidamente descartada; os comandos de dispensa só serão possíveis após a troca da primeira chave;

17.27. A solução de criptografia oferecida deve permitir a troca da chave previamente gravada em fábrica através de processo remoto, via rede, com uso de chave cadastrada para esse processo; devem ser fornecidos os softwares, aplicativos e outras ferramentas necessárias à essa operação;

17.28. O mecanismo do depósito em espécie deve permitir a realização de depósito sem uso de envelopes com crédito em tempo real em contas do Banco do Nordeste do Brasil seguindo os padrões universais de segurança e tecnologia;

17.29. O módulo deverá identificar e reconhecer a denominação do valor facial, validar a autenticidade durante as operações de depósito de todas as cédulas brasileiras de Real (R$), através da análise de um ou mais dos seguintes itens:

17.29.1. Elementos de segurança;

17.29.2. Propriedades do papel;

17.29.3. Propriedades fluorescentes do papel;

17.29.4. Propriedades das tintas de impressão e das tintas magnéticas.

17.30. O índice de rejeição de cédulas autênticas deverá ser de no máximo 5%;

17.31. Deverá possuir os seguintes componentes:

17.31.1. Escrow de no mínimo 1 cédula;

17.31.2. Empilhador/cassete fechado com capacidade de depósito para no mínimo 1.000 cédulas;

17.31.3. Detecção de cédulas entintadas;

17.31.4. O módulo não deverá aceitar as cédulas depositadas com áreas entintadas acima de 10%.

17.32. Deve receber depósito em espécie, em maço solto de 01(uma) até, no mínimo, 30 (trinta) cédulas, de uma única vez;

17.33. Deve receber depósito em maço com as cédulas posicionadas em qualquer face, inclusive misturadas;

17.34. O módulo dever ser capaz de ser configurado para reconhecimento de novas versões e denominações de cédulas lançadas pelo Bancos Central do Brasil;

17.35. Deve devolver as cédulas não validadas;

17.36. Deve validar as cédulas em operações de depósito;

17.37. Deve rejeitar as cédulas não validadas e consideradas como cédulas presumivelmente falsas, devolvendo-as ao usuário durante a operação de depósito;

17.38. Deve rejeitar as cédulas fora de especificação, ou seja, não utilizáveis, dilaceradas e mutiladas, conforme orientação do BACEN, depositadas pelo usuário;

17.39. Deve possui, no mínimo, sensores (implementados por hardware ou software) para identificação de:

17.39.1. Empilhador quase cheio;

17.39.2. Empilhador cheio;

17.39.3. Empilhador fora de posição ou ausente, com indicação sonora e/ou visual de sua presença;

17.39.4. Cédulas enroscadas, com localização aproximada;

17.39.5. Mecanismo de tracionamento/transporte de cédulas fora de posição;

17.39.6. Erros mecânicos durante o processamento;

17.39.7. Presença de cédulas no bocal de depósito.

17.40. Deve suportar contadores de cassetes que aumentam (depósito) e diminuem (saque) dinamicamente;

17.41. A aplicação deve monitorar cassetes recicláveis para evitar "fora de serviço" quando um cassete encher ou esvaziar;

17.42. A aplicação deve informar quando o(s) cassete(s) de rejeição/depósito estiver(em) cheio(s), enviando dados para que sejam adotados procedimentos para alívio manual do(s) cassete(s).

18. SISTEMA DE ENTINTAMENTO DE CÉDULAS

18.1. O sistema de entintamento de cédulas deve ser constituído de recipientes para tintas que deverão ser instalados no interior de cada cassete ATM;

18.2. O módulo de acionamento do sistema deve ser passivo;

18.3. Os recipientes de tinta deverão resistir aos agentes químicos e físicos presentes na composição da tinta, além de garantir a sua fragmentação e o espalhamento da tinta sobre

as cédulas contidas no interior dos cassetes, no ato da explosão ou movimento brusco, de característica similar ao de uma explosão;

18.4. Os recipientes de tinta não deverão apresentar qualquer tipo de alteração em sua constituição devido aos componentes da tinta por no mínimo 2 (dois) anos;

18.5. Os recipientes de tinta deverão ter sua estanqueidade garantida, de modo a não causar vazamentos indevidos;

18.6. Os recipientes de tinta devem ter sido desenvolvidos considerando o projeto original dos cassetes não sendo admitidas adaptações que possam interferir no funcionamento pleno desses nem na sua capacidade de cédulas;

18.7. As tintas deverão ser fornecidas por empresas idôneas, especializadas na fabricação de tintas para impressão de cédulas de dinheiro;

18.8. A tinta deve ser na cor vermelha;

18.9. A tinta deve apresentar forte poder de impregnação, resistindo à ação de agentes químicos ou físicos, tais como solventes orgânicos, água, ácidos, bases, agentes oxidantes, agentes combinados, raspagens etc., que visem suprimir ou reduzir a evidência de entintamento;

18.10. A tinta deve possuir certificação RoHS (Restrição de Substâncias Perigosas) ou sua equivalente brasileira; em caso de descarte, não deve contaminar o meio ambiente.

19. ESPELHOS DE SEGURANÇA

19.1. Devem possuir no mínimo 135mm de largura por 35mm de altura;

19.2. Devem ser convexos, permitindo um ângulo de visão adequado para a segurança do usuário;

19.3. Devem ser posicionados no do gabinete superior, permitindo que o usuário do ATM visualize os arredores;

19.4. Devem ser resistentes, de forma a não permitir a sua remoção.

20. ALARMES DE SENSORES

20.1. CARACTERÍSTICAS GERAIS

20.1.1. O ATM deve emitir sinal sonoro ao ser inicializado;

20.1.2. Os sensores e dispositivos deverão ser controlados por módulos de hardware e software com as seguintes características:

20.1.2.1. Alimentados por bateria de chumbo do tipo selada, com alta resistência a vazamentos ou bateria de lítio. A bateria deve garantir no mínimo 96 (noventa e seis) horas de funcionamento contínuo sem alimentação externa;

20.1.2.2. A bateria deve ser instalada no interior do cofre do equipamento;

20.1.2.3. Devem possuir fonte independente para alimentação do sistema de supervisão dos sensores, de forma que o sistema não seja interrompido quando do desligamento total do equipamento;

20.1.2.4. A comunicação com o módulo deve ser feita por meio da interface de teclado ou porta serial ou *Universal Serial BUS* (USB);

20.1.2.5. Deve disponibilizar contato seco para conexão com a central de alarme;

20.1.2.6. Deve gravar *log* de, no mínimo, 80 (oitenta) eventos;

20.1.2.7. O sistema deve registrar no mínimo 5.000 eventos, com garantia de integridade via mecanismos de assinatura ou *hashing* criptográfico. Os logs devem ser exportáveis de forma criptografada para o sistema central de monitoramento.

20.1.2.8. Deve possuir conectividade total com a API do fabricante do equipamento, objetivando garantir que o sistema do CONTRATANTE receberá as informações enviadas pelos sensores e dispositivos.

20.1.3. Deve possibilitar que todos os sensores estejam integrados ao microcomputador, através da interface de alarmes, para monitoração centralizada de ocorrências.

20.1.4. Todos os eventos do ATM — incluindo logs de segurança, auditoria de firmware, tentativas de acesso, eventos de sensores e operações criptográficas — devem ser exportáveis em formato estruturado (JSON, syslog ou equivalente) por canal seguro utilizando TLS 1.2 ou superior. Os logs devem ser assinados digitalmente e possuir mecanismos de proteção contra exclusão ou modificação não autorizada (tamper-evident).

20.2. **SENSORIAMENTO DO GABINETE**

20.2.1. 01 (um) detector de fumaça;

20.2.2. 02 (dois) sensores de temperatura;

20.2.3. 02 (dois) detectores de vibração;

20.2.4. 02 (dois) sensores de porta trancada, sendo um na fechadura e outro no segredo;

20.2.5. 01 (um) sensor sísmico;

20.2.6. 01 (um) sensor de nível capaz de detectar o desnivelamento do ATM durante a tentativa de remoção;

20.2.7. Sensores que permitam monitorar a abertura do painel frontal;

20.2.8. Sensores que permitam monitorar a abertura da porta traseira;

20.2.9. Sensores que permitam monitorar a violação do painel do operador tal como a retirada do dispositivo.

20.3. **LEITOR DE CARTÕES**

20.3.1. Sensor e dispositivo *Anti Skimming* objetivando identificar a instalação, sobre o leitor de cartões, de qualquer artefato de captura de informações do cartão, conforme subitem 22.9;

20.3.2. Sensores que permitam monitorar o arrancamento do leitor de cartões.

20.4. CASSETES

20.4.1. Os cassetes para cédulas regulares e rejeitadas devem possuir sensores integrados por software, o software deve ser fornecido;

20.4.2. Os cassetes para cédulas regulares e rejeitadas devem possuir sensores que possibilitem identificar as seguintes situações:

20.4.2.1. *Shutter* aberto;

20.4.2.2. Detecção de cédulas duplas e fora de especificação, de forma dinâmica, ou seja, a verificação das características físicas das cédulas (espessura e largura) deve ser realizada a cada pagamento;

20.4.2.3. Quase fim de cédulas. No caso de ausência de sensor específico de quase fim de cédulas, este sensoriamento poderá ser obtido por software mediante o confronto de um limite mínimo de cédulas estabelecido pelo aplicativo do CONTRATANTE com a quantidade de cédulas disponível em cada cassete, cujo cálculo deve considerar, além das cédulas efetivamente dispensadas, aquelas rejeitadas pelo equipamento;

20.4.2.4. Fim de cédulas. No caso de ausência de sensor específico de fim de cédulas, este sensoriamento poderá ser obtido por software a partir da combinação do sensor de quase fim de cédulas e falha de alimentação simultaneamente;

20.4.2.5. Cassetes fora da posição correta, ausentes ou mal encaixados;

20.4.2.6. Sensor de presença para identificar cédulas, no bocal, no *presenter* e na balança, que ficaram “presas” dentro da ATM, ou seja, cédulas que não foram dispensadas para o cliente na transação;

20.4.2.7. Sensor de cassetes ausentes.

20.5. MÓDULO PARA DEPÓSITO E PAGAMENTO DE CÉDULAS

20.5.1. O módulo para depósito e pagamento de cédulas deve possuir sensores que possibilitem identificar, no mínimo, as seguintes situações:

20.5.1.1. Abertura da entrada;

20.5.1.2. Cassete cheio;

20.5.1.3. *Shutter* aberto.

20.6. MONITOR DE VÍDEO

20.6.1. O monitor deve possuir sensor que identifique se ele foi sobreposto, desconectado e/ou removido;

20.6.2. O monitor deve contar com sensor que ajuste automaticamente a intensidade do brilho, em função da variação de luminosidade do ambiente (ainda que sob luz solar direta), permitindo a visualização adequada da tela, sem que haja excesso ou falta de brilho.

20.7. FONE DE OUVIDO

20.7.1. Sensor que indique a presença de fone de ouvido para dar suporte aos recursos de acessibilidade a portadores de necessidades especiais.

20.8. SENSOR SÍSMICO

20.8.1. Deve ser capaz de detectar ataques com explosivo, tentativa de violação com ferramentas de pressão hidráulica, martelos, furadeiras de impacto, brocas diversas, equipamentos de corte com discos e abrasivos, lanças térmicas, maçaricos de corte, lança de oxigênio, laser de corte etc.

20.9. SENSOR ANTISKIMMING

20.9.1. Deve ser capaz de detectar e reagir a artefatos espúrios sobrepostos à área do leitor de cartões ou inseridos no leitor de cartões, com o intuito de capturar dados e retenção dos cartões;

20.9.2. Os sensores deverão ser instalados internamente à leitora e/ou painel frontal;

20.9.3. Não deverão ser alteradas as características externas do painel frontal ou da leitora, bem como suas funcionalidades;

20.9.4. Deve ter inteligência autônoma embarcada, que permita o perfeito atendimento dos recursos definidos neste Edital;

20.9.5. O sistema deve ser compatível e interagir com a API do fabricante do ATM, de forma a garantir que o CONTRATANTE possa receber as informações enviadas pelo dispositivo *antiskimming*;

20.9.6. Deve detectar e reagir a ataques a qualquer dos componentes do sistema, inclusive a desconexões ou cortes de cabos;

20.9.7. Deve detectar a colocação de peças metálicas, plásticas ou de outros materiais que possam ser utilizados nos ataques, ainda que de pequeno porte;

20.9.8. Ao ser acionado, o sistema deve disparar trava mecânica que impeça a inserção de cartões na leitora;

20.9.9. Deve permitir ajustes no nível de sensibilidade dos sensores, de maneira a permitir correções para evitar alarmes falsos;

20.9.10. Deve permitir ajustes no tempo de reação, considerando a permanência do artefato espúrio, de segundo em segundo;

20.9.11. O tempo de reação padrão, configurado em fábrica, deve ser de 240 (duzentos e quarenta) segundos (4 minutos); nas tentativas de ataque aos componentes do dispositivo ou com a detecção de artefatos espúrios; decorrido o tempo definido para reação, o sistema deve agir, provocando o acionamento de alarme sonoro e o disparo da trava mecânica;

20.9.12. Caso seja retirado o objeto espúrio, o sistema deve retomar as funções do ATM, desbloqueando a leitora e cessando o alarme sonoro;

20.9.13. O sistema deve permanecer ativo mesmo com o ATM desligado ou fora da rede, para isso deve contar com bateria, compatível com as necessidades dos componentes.

20.10. **INTERFACE DA CENTRAL DE ALARMES**

20.10.1. Deve estar localizada dentro do cofre;

20.10.2. Deve ser capaz de receber os sinais dos sensores, gerando, para a CPU do ATM, alerta individual de cada sensor para monitoração remota e adoção de medidas;

20.10.3. Em caso de corte de energia elétrica do equipamento, a interface deve enviar um sinal para a central de monitoramento;

20.10.4. Deve possuir entrada para leitura de todos os sensores do ATM;

20.10.5. Deve possuir entrada para instalação de sirene;

20.10.6. As comunicações seriais deverão possuir isoladores elétricos com acoplamento óptico, a fim de proteger os equipamentos interligados ao ATM;

20.10.7. Deve ser capaz de utilizar a fonte de alimentação por baterias do conjunto.

21. SUSTENTABILIDADE AMBIENTAL

21.1. Deve ser preferencialmente acondicionado em embalagem individual adequada, com o menor volume possível, que utilize materiais recicláveis, de forma a garantir a máxima proteção durante o transporte e o armazenamento;

21.2. Pelo menos 80% dos componentes dos equipamentos devem possuir Certificado de Rotulagem Ambiental, emitido pela ABNT, ou certificado emitido por organismo acreditado pela Coordenação Geral de Acreditação (CGCRE/INMETRO), que assegure a conformidade com a Diretiva ROHS ou Autodeclaração de conformidade emitida pela organização atestando a conformidade com a Diretiva ROHS.