

ANEXO I-A**ESPECIFICAÇÕES TÉCNICAS****1. EQUIPAMENTOS E SOFTWARES****1.1. CAMERA IP FIXA DOME COM CARTÃO DE MEMÓRIA E BASE DE FIXAÇÃO**

- 1.1.1. Deverá ser adequada para uso em ambiente interno e externo.
- 1.1.2. Deverá ser do tipo fixa dome colorida.
- 1.1.3. Deverá ser do tipo IP nativo, não sendo permitida a utilização de conversores, encoders ou dispositivos externos.
- 1.1.4. Deverá possuir sensor de imagem de 1/3" ou superior, com varredura progressiva.
- 1.1.5. Deverá possuir iluminador infravermelho (IR) com alcance mínimo de 30 (trinta) metros.
- 1.1.6. Deverá possuir lente varifocal de 2,8, no máximo, a 12 mm, no mínimo, ou equivalente que assegure ângulo de abertura horizontal entre 40° a 100° e abertura vertical entre 25° a 50°.
- 1.1.7. Deverá possuir sensibilidade luminosa mínima de 0,01 lux (modo colorido) e 0 lux com IR ativado.
- 1.1.8. Deverá possuir função Day/Night com filtro de corte infravermelho (ICR).
- 1.1.9. Deverá possuir WDR (Wide Dynamic Range) real com, no mínimo, 100 dB.
- 1.1.10. Deverá possuir função BLC (Compensação de Luz de Fundo).
- 1.1.11. Deverá possuir função AGC (Controle Automático de Ganho).
- 1.1.12. Deverá possuir função DNR (Redução Digital de Ruído);
- 1.1.13. Deverá possuir analíticos de vídeo embarcados com capacidade de geração de alarmes para, no mínimo, os seguintes eventos: detecção de movimento, cruzamento de linha, alteração da condição da cena, entrada em área por tempo, aglomeração de pessoas, objeto abandonado e objeto removido.
- 1.1.14. Deverá possuir função de máscara de privacidade configurável.
- 1.1.15. Deverá permitir compressão de vídeo, no mínimo, nos formatos MJPEG e H.265.
- 1.1.16. Deverá permitir a transmissão simultânea de, no mínimo, 3 (três) streams de vídeo, sendo, pelo menos, 2 (dois) streams em resolução 1920 × 1080 pixels a 30 frames por segundo.
- 1.1.17. Deverá permitir acesso de visualização simultânea para, no mínimo, 5 (cinco) usuários.
- 1.1.18. Deverá possuir controle de acesso por usuário e senha, com diferentes níveis de permissão.
- 1.1.19. Deverá possuir interface de rede Ethernet 100 Mbps, com conector RJ-45.

- 1.1.20. Deverá possuir servidor web embarcado para visualização via navegador, compatível com, no mínimo, duas das seguintes plataformas: Microsoft Edge, Google Chrome ou Mozilla Firefox.
- 1.1.21. Deverá possuir alimentação via PoE (Power over Ethernet), conforme padrão IEEE 802.3af ou superior.
- 1.1.22. Deverá possuir suporte aos protocolos IPv4, IPv6, UDP, TCP, HTTP, HTTPS, RTP, ICMP, RTSP, FTP, DHCP, DNS, SMTP, NTP, SNMP e QoS, no mínimo.
- 1.1.23. Deverá possuir suporte ao padrão aberto ONVIF.
- 1.1.24. Deverá possuir grau de proteção IP66 e IK10, no mínimo.
- 1.1.25. Deverá possuir temperatura de operação mínima de até 50 °C.
- 1.1.26. Deverá possuir, no mínimo, 1 (uma) entrada e 1 (uma) saída de áudio.
- 1.1.27. Deverá possuir, no mínimo, 1 (uma) entrada e 1 (uma) saída de alarme.
- 1.1.28. Deverá possuir slot para cartão de memória que permita a gravação local de imagens.
- 1.1.29. Deverá ser fornecida com cartão de memória de no mínimo 128 GB, Classe 10 ou superior, com velocidade mínima de gravação de 10 MB/s.
- 1.1.30. Deverá ser fornecida com base de fixação para parede ou teto, adequada ao acondicionamento de cabos e conectores.
- 1.1.31. Deverá ser fornecida com o firmware mais recente disponibilizado pelo fabricante.
- 1.1.32. Deverá ser compatível com o software de CFTV IP especificado neste Anexo.

1.2. SWITCH DE REDE DE 24 PORTAS

- 1.2.1. Deverá possuir LEDs indicativos do estado de funcionamento do equipamento.
- 1.2.2. Deverá possibilitar a coleta de estatísticas de tráfego e de falhas para todas as portas.
- 1.2.3. Deverá permitir a reconfiguração dinâmica das portas e módulos, incluindo ativação e desativação, de portas e módulos, sem necessidade de reinicialização e sem causar instabilidade ou impacto no funcionamento do equipamento.
- 1.2.4. Deverá implementar ajuste e sincronização de relógio via NTP (Network Time Protocol).
- 1.2.5. Deverá permitir o envio de logs para servidores remotos, por meio do protocolo Syslog.
- 1.2.6. Deverá implementar a funcionalidade traceroute, permitindo o descobrimento do caminho percorrido por pacotes na rede.
- 1.2.7. Todas as portas deverão ser autoconfiguráveis MDI/MDIX, dispensando o uso de cabos cross-over ou qualquer configuração para conexão a outro switch.
- 1.2.8. Deverá permitir que um conjunto de switches seja administrado por um único endereço IP.
- 1.2.9. O conjunto deverá suportar no mínimo 8 (oito) switches operando de forma integrada.

- 1.2.10. Deverá suportar protocolos seguros para cópia de arquivos de configuração, sendo aceitos Secure Copy Protocol (SCP) ou Secure File Transfer Protocol (SFTP).
- 1.2.11. Deverá implementar gerenciamento conforme padrão SNMP (Simple Network Management Protocol), com suporte à RFC 1213 (MIB-II) e SNMP v3.
- 1.2.12. Deverá suportar configuração NETCONF ou Provisionamento Zero-Touch (ZTP) através do software de gerenciamento.
- 1.2.13. Deverá permitir a monitoração de desempenho de tráfego via MIB SNMP.
- 1.2.14. Deverá implementar espelhamento de portas (Port Mirroring) para análise local ou remota de tráfego em portas de uma mesma VLAN.
- 1.2.15. Deverá suportar os protocolos LLDP (Link Layer Discovery Protocol) e LLDP-MED (LLDP for Media Endpoint Devices), conforme padrões IEEE.
- 1.2.16. Deverá possuir 1 (uma) porta de gerenciamento out-of-band, podendo ser porta serial ou porta lógica isolada por VLAN.
- 1.2.17. Deverá permitir o gerenciamento via Command Line Interface (CLI).
- 1.2.18. Deverá permitir o gerenciamento por interface web com suporte a SSL (Secure Socket Layer) versão 3 e SSH (Secure Shell) versão 2.
- 1.2.19. Deverá permitir o gerenciamento via TELNET.
- 1.2.20. Deverá permitir autenticação centralizada por meio de RADIUS ou TACACS+, ou padrão compatível.
- 1.2.21. Deverá permitir instalação em rack padrão de 19", ocupando 1U, devendo ser fornecidos todos os acessórios necessários à fixação.
- 1.2.22. Deverá possuir a capacidade mínima de encaminhamento de 80 milhões de pacotes por segundo (pacotes de 64 bytes), em camada 2 ou 3, quando aplicável (modelo de referência OSI).
- 1.2.23. A matriz de comutação (Switch Fabric) deverá possuir throughput mínimo de 100 Gbps.
- 1.2.24. As memórias DRAM e Flash deverão ser dimensionadas pelo fabricante para suportar o sistema operacional, logs, firmware, recursos de gerenciamento e atualizações, sem limitação funcional.
- 1.2.25. Deverá suportar interfaces 10/100/1000 Mbps RJ-45, para cabos UTP categoria 6 ou superior, full duplex, autosense, conforme os padrões: IEEE 802.3 (10Base-T), IEEE 802.3u (100Base-TX) e IEEE 802.3ab (1000Base-T).
- 1.2.26. Deverá possuir no mínimo 12 (doze) portas RJ-45 Gigabit Ethernet instaladas.
- 1.2.27. Deverá possuir no mínimo 2 (dois) slots SFP Gigabit LC, sendo fornecidos 2 transceivers SFP multimodo.
- 1.2.28. O gerenciamento via porta de gerenciamento ou console deverá possuir processo de autenticação e identificação positiva.
- 1.2.29. Deverá permitir a criação de ACLs baseadas em endereço IP para controle de acesso via Telnet e SSH.

- 1.2.30. Deverá implementar autenticação de login/senha para a liberação de tráfego na porta via protocolo IEEE 802.1x com as seguintes funcionalidades: atribuição de VLAN conforme a autenticação do usuário; reautenticação forçada de todas as portas, reautenticação periódica e definição de período de inatividade após falha de autenticação.
- 1.2.31. Deverá implementar ACLs baseadas em portas físicas.
- 1.2.32. Deverá suportar ACLs baseadas em tempo.
- 1.2.33. Deverá implementar segurança de portas com distinção entre interfaces confiáveis e não confiáveis, mantendo correlação entre porta, VLAN, IP e MAC (ex.: DHCP Snooping).
- 1.2.34. Deverá implementar AAA (Authentication, Authorization and Accounting) com garantia de entrega dos pacotes.
- 1.2.35. Todo o tráfego de controle administrativo deverá ser devidamente contabilizado.
- 1.2.36. O tráfego administrativo deverá utilizar protocolo TCP, visando maior confiabilidade.
- 1.2.37. Deverá permitir autenticação mútua entre o servidor e cliente AAA.
- 1.2.38. Deverá implementar proteção contra o recebimento de BPDUs inesperadas nas portas de acesso.
- 1.2.39. Deverá permitir limitação da quantidade de endereços MAC por porta.
- 1.2.40. Deverá suportar a visualização de endereços MAC aprendidos.
- 1.2.41. Deverá realizar o aprendizado dinâmico de MAC, reconhecendo movimentações sem intervenção manual.
- 1.2.42. Deverá permitir vinculação estática de endereço MAC a porta específica.
- 1.2.43. Deverá permitir controle de broadcast por porta, compatível com IPv4 e IPv6, sem uso de ACL.
- 1.2.44. Deverá disponibilizar API de gerenciamento remoto, baseada em padrões abertos REST, RESTCONF, NETCONF ou equivalente, documentada pelo fabricante e com autenticação segura.
- 1.2.45. As capacidades mínimas de VLAN, MAC address, ACLs, SNMP, espelhamento e QoS deverão ser suportadas de forma simultânea, sem degradação de desempenho.
- 1.2.46. Deverá suportar os seguintes protocolos e padrões: IEEE 802.3, 10BaseT; IEEE 802.3u, 100BaseTX; IEEE 802.3ab, 1000BaseT; IEEE 802.3x, Flow Control; IEEE 802.1q, VLAN Tagging; IEEE 802.1d, SpanningTree; IEEE 802.1s, Multiple Spanning Tree; IEEE 802.3ad, Link Aggregation; IEEE 802.1x, Port-Level Security; IEEE 802.1w, Rapid Spanning Tree.
- 1.2.47. Deverá implementar mecanismos de rápida convergência de Spanning Tree, incluindo Root Guard e BPDU Protection.
- 1.2.48. Deverá suportar BPDU Guard e BPDU Filter, com opção de reativação automática das portas.
- 1.2.49. Deverá suportar quadros Ethernet jumbo com tamanho de, no mínimo, 4.000 bytes.

- 1.2.50. Deverá suportar no mínimo 4.000 VLANs.
- 1.2.51. Deverá implementar trunking IEEE 802.1Q, com negociação automática.
- 1.2.52. Cada porta deverá possuir mínimo de 4 filas, com suporte a WRR, SRR ou equivalente.
- 1.2.53. Deverá permitir classificação de tráfego conforme IEEE 802.1p.
- 1.2.54. Deverá suportar no mínimo 8.000 endereços MAC simultâneos.
- 1.2.55. Deverá suportar agregação de enlaces conforme IEEE 802.3ad em todas as portas.
- 1.2.56. Deverá implementar o LACP (Link Aggregation Control Protocol).
- 1.2.57. Deverá suportar IGMP Snooping versões 1, 2 e 3.
- 1.2.58. Deverá suportar no mínimo 128 grupos multicast IGMP.
- 1.2.59. Deverá implementar DHCP Snooping e DHCP Server.
- 1.2.60. Deverá possuir fonte interna bivolt automática (110–220 V, 50/60 Hz).
- 1.2.61. Deverá possuir ventilação ativa com controle inteligente de velocidade.
- 1.2.62. Deverá ser compatível com as câmeras IP especificadas neste Anexo.
- 1.2.63. O switch deverá possuir capacidade total de fornecimento de potência PoE (Power over Ethernet) dimensionada para suportar simultaneamente as câmeras IP previstas neste Anexo, considerando o consumo máximo por câmera em regime contínuo de operação (incluindo iluminador infravermelho, WDR, analíticos embarcados, gravação local em cartão de memória e demais funcionalidades ativas), sem degradação de desempenho, instabilidade elétrica ou limitação operacional.

1.3. SERVIDOR DE CFTV IP COM ARMAZENAMENTO DE 24 TB

- 1.3.1. Deverá ser um equipamento dedicado e desenvolvido especificamente para a função de servidor de gravação de CFTV, com capacidade para a operação ininterrupta e com alta carga computacional.
- 1.3.2. O servidor deverá possuir processador em linha de produção com, no mínimo, os seguintes parâmetros: 5,0 GHz de frequência máxima, no mínimo; 12 núcleos físicos, no mínimo; 20 threads, no mínimo; e 24 MB de memória cache, no mínimo.
- 1.3.3. Deverá possuir memória RAM de, no mínimo, 32 GB, com capacidade de expansão para, no mínimo, até 64 GB, sem substituição dos módulos existentes.
- 1.3.4. Deverá possuir gabinete compatível com rack padrão de 19 (dezenove) polegadas.
- 1.3.5. A altura do servidor deverá ser, no máximo, 4U (quatro unidade de rack).
- 1.3.6. Deverá ser fornecido com sistema operacional Microsoft Windows 11 ou superior, visando compatibilidade com o ambiente computacional do BANCO.
- 1.3.7. A versão do sistema operacional do servidor deverá permitir acesso e administração remota, por meio de ferramenta nativa do próprio sistema.
- 1.3.8. Deverá permitir a instalação, execução e atualização do software antivírus Palo Alto Cortex, utilizado pelo BANCO, sem restrições de compatibilidade ou desempenho.

- 1.3.9. Deverá permitir a integração com o serviço de domínio do Microsoft Active Directory (AD), utilizado pelo BANCO, incluindo autenticação e gerenciamento centralizado.
- 1.3.10. Deverá possuir unidade de estado sólido (SSD) dedicada ao sistema operacional e aos aplicativos do sistema de CFTV IP, dimensionada pelo CONTRATADO para garantir desempenho, estabilidade e vida útil adequada ao regime contínuo de operação.
- 1.3.11. Deverá possuir, no mínimo, 2 (duas) saídas de vídeo, sendo 1 (uma) HDMI e 1 (uma) VGA, DVI ou DisplayPort.
- 1.3.12. Deverá possuir, no mínimo, 3 (três) portas USB, no mínimo.
- 1.3.13. Deverá possuir, no mínimo, 2 (duas) interfaces de rede Ethernet RJ-45 Gigabit.
- 1.3.14. Deverá possuir, no mínimo, 1 (uma) saída de áudio.
- 1.3.15. Deverá possuir armazenamento em disco rígido (HDD) com capacidade mínima bruta total de 24 TB, constituído por 2 discos de 12 TB, com as seguintes características: interface SATA 6 Gb/s, velocidade mínima de 7.200 RPM e capacidade de expansão par, no mínimo, até 40 TB. Os discos rígidos deverão ser específicos e homologados para aplicações de CFTV, não sendo aceitos equipamentos de uso convencional para computadores pessoais.
- 1.3.16. O CONTRATADO deverá dimensionar o armazenamento do servidor, de forma a suportar a retenção de até 60 (sessenta) dias de gravação, considerando as seguintes características: quantidade média de 28 de câmeras por unidade, sendo no mínimo 6 e no máximo 68 câmeras por unidade, resolução 1920 x 1080 pixels, compressão H.265, velocidade de 15 frames por segundo e gravação baseada em detecção de movimento.
- 1.3.17. Deverá possuir 2 fontes de alimentação redundantes com tensão elétrica nominal de 110V a 220 VAC, frequência 50/60Hz e seleção automática.
- 1.3.18. A fonte de alimentação deverá ser dimensionada pelo CONTRATADO para suportar a carga exigida pelo servidor em regime contínuo.
- 1.3.19. O servidor deverá possuir slot de expansão compatível para instalação futura de unidade de processamento gráfico dedicada (GPU).
- 1.3.20. O servidor de CFTV IP deverá ser compatível com o software de CFTV IP especificado neste Anexo, incluindo suas funcionalidades, módulos e analíticos de inteligência artificial.

1.4. SOFTWARE DE CFTV IP

- 1.4.1. O software de CFTV IP deverá possuir licenciamento de uso permanente para **89 servidores de CFTV e 2.472 câmeras IP** distribuídas em **89 unidades** do BANCO. O software de CFTV IP deverá ser obrigatoriamente da marca **ISS**, em razão da padronização tecnológica, interoperabilidade e compatibilidade com o sistema de CFTV já implantado em 226 (duzentas e vinte e seis) unidades do BANCO (**versões SecurOS Premium e SecurOS MCC Direct Connect**), de forma a assegurar continuidade operacional, integração sistêmica, unificação da plataforma de gestão e redução de riscos operacionais e de segurança. As licenças destinadas aos analíticos de reconhecimento facial e detecção de volumes poderão ser utilizadas em quaisquer câmeras IP da Unidade, conforme definição e conveniência do BANCO.

- 1.4.2. Deverá possuir plataforma/arquitetura aberta que permita a utilização de câmeras IP de diferentes fabricantes, com, no mínimo e simultaneamente, as seguintes funções: visualização ao vivo, gravação, reprodução, cópia de segurança (backup), transmissão remota e integração de analíticos de vídeo embarcados.
- 1.4.3. Deverá suportar a integração com aplicações de terceiros, de forma nativa ou nativamente ou através de interfaces de integração (API), com, no mínimo, as seguintes funções: exibição de imagens ao vivo, reprodução de gravações, busca por período e busca por movimento.
- 1.4.4. As APIs e as ferramentas de desenvolvimento (SDK) deverão ser disponibilizadas para o BANCO sem custo adicional, incluindo a documentação de integração.
- 1.4.5. Deverá operar no sistema operacional disponível nos servidores de CFTV especificados neste Anexo, visando compatibilidade com o ambiente computacional do BANCO.
- 1.4.6. Deverá operar como um serviço nativo real do sistema operacional do servidor de CFTV, iniciando automaticamente após a reinicialização do servidor.
- 1.4.7. A comunicação entre o software e as câmeras IP deverá ocorrer em tempo real, utilizando exclusivamente a rede corporativa do BANCO.
- 1.4.8. A gravação das imagens deverá ser descentralizada e local, realizada no servidor de CFTV de cada unidade do BANCO, independentemente da disponibilidade de comunicação com a Central de Segurança.
- 1.4.9. Deverá possuir ferramenta de configuração global de câmeras, permitindo a aplicação simultânea de parâmetros comuns a grupos de câmeras, incluindo, no mínimo: parâmetros de gravação, resolução, taxa de quadros, detecção de movimento e analíticos.
- 1.4.10. Deverá possibilitar o acesso remoto ao sistema, permitindo a visualização das imagens ao vivo, reprodução de vídeo e configuração por meio de software cliente.
- 1.4.11. Deverá suportar, no mínimo, 10 (dez) clientes remotos simultâneos na Central de Segurança do BANCO.
- 1.4.12. Deverá possuir suporte ao padrão aberto ONVIF.
- 1.4.13. O sistema deverá ter por idioma padrão em todas as interfaces a Língua Portuguesa do Brasil.
- 1.4.14. Deverá suportar câmeras com, no mínimo, 3 (três) streams de vídeo, permitindo configurações independentes para visualização, gravação e detecção de movimento.
- 1.4.15. Deverá permitir a configuração dos streams de vídeo das câmeras IP de diferentes fabricantes diretamente pela interface do software de CFTV.
- 1.4.16. Deverá possuir servidor web integrado para acesso das imagens através de navegador de Internet.
- 1.4.17. Deverá permitir a conexão a múltiplos servidores para visualização remota de até 64 canais ao mesmo tempo.
- 1.4.18. Deverá ter capacidade de gravação em resoluções de 2 a 4 Megapixels, no mínimo.
- 1.4.19. Deverá permitir gravação das imagens usando, no mínimo, os formatos MJPEG, H.264 e H.265.

- 1.4.20. Deverá suportar taxa de até 30 (trinta) quadros por segundo (fps) para gravação e visualização ao vivo, por câmera.
- 1.4.21. Deverá permitir a configuração de imagens por segundo, resolução e qualidade para cada câmera individualmente.
- 1.4.22. Deverá suportar configuração de armazenamento remoto das imagens.
- 1.4.23. Deverá permitir backup e restauração das configurações do sistema.
- 1.4.24. O sistema deverá permitir a configuração por gravação contínua, eventos de dispositivos externos, por faixa de horário e detecção de movimento.
- 1.4.25. Deverá permitir a retenção das gravações de vídeo com base na parametrização do número de dias definido pelo usuário.
- 1.4.26. Deverá permitir a sincronização automática das gravações disponíveis no cartão de memória das câmeras IP, no caso de falha na gravação local do servidor.
- 1.4.27. Deverá possuir recurso para autenticação da integridade das imagens gravadas.
- 1.4.28. Deverá suportar o arquivamento das gravações em mídias removíveis.
- 1.4.29. Deverá suportar gravação por agendamento, permitindo a definição de horários e dias com diferentes modos de gravação.
- 1.4.30. Deverá permitir a configuração de múltiplas zonas de detecção de movimento por câmera.
- 1.4.31. O sistema deverá permitir pré-gravação e gravação pós-evento.
- 1.4.32. Deverá permitir a reprodução sincronizada de múltiplas câmeras simultaneamente.
- 1.4.33. Deverá possuir métodos de pesquisa por movimento e por tempo.
- 1.4.34. Deverá permitir a geração de "snapshot" das imagens gravadas, contendo data e hora do evento.
- 1.4.35. Deverá permitir a exportação de vídeo nos formatos AVI ou MP4, no mínimo.
- 1.4.36. Deverá permitir a exportação de imagens no formato JPEG, no mínimo.
- 1.4.37. Deverá permitir a impressão de imagens contendo data e hora da gravação.
- 1.4.38. Deverá permitir a utilização do recurso de zoom digital em imagens ao vivo.
- 1.4.39. Deverá permitir autenticação de usuários via Microsoft Active Directory (AD).
- 1.4.40. Deverá permitir a criação de usuários e grupos, com atribuições de permissões.
- 1.4.41. Deverá permitir a aplicação de níveis de permissão por objeto do sistema (servidor, câmeras, clientes).
- 1.4.42. Deverá possuir registro de eventos (log), contemplando todas as ações de usuários e operações do sistema.
- 1.4.43. Os logs deverão ser armazenados em banco de dados, com retenção de 12 (doze) meses, no mínimo.

- 1.4.44. Deverá gerar alarme quando do acionamento de dispositivos externos interligados nas entradas digitais das câmeras IP.
- 1.4.45. Deverá gerar alarme quando da ocorrência de detecção de movimento de câmeras em horários pré-definidos.
- 1.4.46. Deverá gerar alarme quando da ocorrência de falha de funcionamento da câmera IP.
- 1.4.47. Deverá permitir a notificação de alarmes por e-mail, utilizando o servidor corporativo de correio do BANCO.
- 1.4.48. Quando da ocorrência de alarmes, o sistema deverá exibir aviso em tela (pop-up) acompanhado de alerta sonoro.
- 1.4.49. Deverá permitir a geração de relatórios de eventos e alarmes, com filtros de data e hora, no mínimo.
- 1.4.50. Deverá permitir o acionamento de saídas de alarme das câmeras IP.
- 1.4.51. Deverá permitir o posicionamento automático de câmeras PTZ, por meio de presets programados, quando da ocorrência de alarmes.
- 1.4.52. Deverá permitir o controle manual de câmeras PTZ por meio de joysticks conectados às estações de monitoramento (clientes).
- 1.4.53. Deverá permitir o controle manual de câmeras PTZ por meio de joystick virtual, utilizando o mouse na interface.
- 1.4.54. Deverá possuir controle de prioridade para operação de PTZ, permitindo a definição de usuário com precedência no comando das câmeras.
- 1.4.55. As ações decorrentes de alarmes deverão ser configuradas individualmente para cada câmera.
- 1.4.56. Deverá possuir mapa sinóptico para visualização e controle dos dispositivos do sistema.
- 1.4.57. Deverá possuir ronda automática de câmeras móveis, por meio de lista de presets, com ajuste de velocidade de movimentação e tempo de permanência em cada preset.
- 1.4.58. O sistema de controle de PTZ deverá permitir ajuste de foco, íris, autofoco e autoíris das câmeras.
- 1.4.59. Deverá permitir a configuração de ações automáticas pré-cadastradas para eventos de alarmes (enviar e-mail, exibir imagem da câmera, tocar som, no mínimo).
- 1.4.60. Deverá permitir monitoramento em tempo real, por meio de ambiente gráfico, das plantas baixas da instalação do sistema de CFTV.
- 1.4.61. Deverá permitir a sincronização automática de data e hora com servidor da rede corporativa do BANCO.
- 1.4.62. Deverá suportar, no mínimo, os seguintes protocolos de rede: TCP/IP, DHCP, DNS, NTP e HTTPS.
- 1.4.63. Deverá permitir comunicação criptografada entre o servidor de gravação e os clientes remotos.

- 1.4.64. Deverá permitir a visualização das imagens por meio de dispositivos móveis compatíveis com as plataformas Android e iOS.
- 1.4.65. Deverá suportar múltiplos monitores de vídeo por estação cliente para o monitoramento ao vivo das imagens.
- 1.4.66. Deverá permitir, a qualquer tempo, a integração de novos modelos de câmeras IP de diferentes fabricantes, de acordo com a necessidade do BANCO.

1.5. ANALÍTICOS DE INTELIGÊNCIA ARTIFICIAL

1.5.1. RECONHECIMENTO FACIAL

- 1.5.1.1. O licenciamento do módulo de reconhecimento facial deverá ser realizado por câmera (stream de vídeo), considerando exclusivamente as câmeras nas quais o analítico estiver efetivamente habilitado.
- 1.5.1.2. Deverá ser considerada a habilitação do analítico de reconhecimento facial em 1 (uma) câmera por servidor, totalizando 89 (oitenta e nove) servidores, perfazendo o quantitativo total de 89 (oitenta e nove) licenças de reconhecimento facial.
- 1.5.1.3. O processamento do analítico de reconhecimento facial deverá ser realizado localmente, ou seja, exclusivamente no servidor de CFTV da unidade, sem qualquer dependência, total ou parcial, de nuvem externa ou de outros servidores da rede interna.
- 1.5.1.4. O treinamento, reprocessamento ou reindexação dos modelos de IA do analítico de reconhecimento facial, se necessário, deverá ser realizado em ambiente computacional do CONTRATADO, considerando que os servidores instalados nas unidades não são dimensionados para essa finalidade.
- 1.5.1.5. O sistema deverá permitir a detecção, captura e reconhecimento facial em tempo real, de múltiplas faces simultaneamente em uma única cena, com processamento baseado em Inteligência Artificial aplicado aos fluxos de vídeo das câmeras IP, desde que atendidos os requisitos mínimos de resolução e densidade de pixels faciais.
- 1.5.1.6. Deverá permitir a configuração de múltiplas zonas de captura facial por câmera, com parâmetros independentes de sensibilidade, ângulo e qualidade mínima da face.
- 1.5.1.7. Deverá realizar a detecção automática do melhor quadro de vídeo para localização e extração de rostos.
- 1.5.1.8. O reconhecimento facial deverá apresentar precisão mínima de 90%, desde que observadas as diretrizes de configuração definidas no sistema.
- 1.5.1.9. Deverá ser capaz de reconhecer uma pessoa com pelos faciais, mesmo que a imagem cadastrada não contenha tal característica.
- 1.5.1.10. Deverá ser capaz de reconhecer uma pessoa usando óculos de grau, ainda que a imagem cadastrada não contenha óculos, desde que não haja obstrução significativa do rosto.
- 1.5.1.11. O sistema deverá desconsiderar automaticamente faces cujo índice de qualidade abaixo do limiar configurado.

- 1.5.1.12. Deverá apresentar indicador de qualidade das faces reconhecidas, para fins de análise posterior.
- 1.5.1.13. Deverá permitir o ajuste os parâmetros de reconhecimento facial.
- 1.5.1.14. Deverá permitir a exibição, na interface do sistema, da taxa de reconhecimento, do nome da pessoa reconhecida e da imagem capturada.
- 1.5.1.15. Deverá suportar a criação e gerenciamento de múltiplos perfis de indivíduos, contendo nome, sobrenome, comentários, múltiplas imagens por pessoa e associação a lista de observação.
- 1.5.1.16. Deverá registrar em banco de dados os metadados completos para cada face capturada, incluindo, no mínimo, a imagem, data, hora e câmera.
- 1.5.1.17. Deverá permitir a importação de faces individualmente ou em lote, desde que atendam aos critérios técnicos mínimos.
- 1.5.1.18. Deverá permitir a inclusão de indivíduos em lista de observação a partir de imagens em grupo, com extração automática de faces de pequeno tamanho.
- 1.5.1.19. Deverá permitir a configuração de eventos, alarmes e ações automáticas com base no reconhecimento de faces vinculadas às listas de observação.
- 1.5.1.20. Deverá disponibilizar ferramentas de busca por pessoa, com base em nome e sobrenome, data, hora, câmera e imagem facial.
- 1.5.1.21. Deverá permitir a pesquisa de rostos no arquivo de vídeo, possibilitando localizar ocorrências de indivíduos previamente cadastrados ou detectados, com base em critérios como imagem facial, período, câmera e local de gravação.
- 1.5.1.22. Deverá permitir a pesquisa forense de rostos no arquivo de vídeo, possibilitando a identificação retrospectiva de indivíduos não previamente cadastrados, por meio de mecanismos avançados de busca e correlação facial em grandes volumes de gravações históricas.
- 1.5.1.23. Deverá permitir a exportação dos logs de eventos de reconhecimento facial.
- 1.5.1.24. Deverá permitir a comparação de um rosto detectado com uma imagem oriunda de cartão de acesso ou base autorizada.
- 1.5.1.25. Deverá permitir a busca no histórico de detecções com base em características faciais, incluindo, no mínimo, cor e comprimento do cabelo, presença de pelos faciais, uso de acessórios, uso de óculos.
- 1.5.1.26. O sistema deverá disponibilizar as API e SDK, permitindo, no mínimo, as seguintes funções: busca, cadastro, atualização, remoção e exportação de faces; busca por similaridade facial; gerenciamento de listas de observação; definição de regras baseadas em reconhecimento facial; e acesso a logs operacionais.
- 1.5.1.27. O reconhecimento facial deverá ser realizado pelo software de CFTV IP instalado nos servidores, de forma independente da existência de analíticos embarcados nas câmeras. As câmeras que possuam detecção de rostos embarcada poderão ser utilizadas como recurso complementar de otimização do processamento, sem prejuízo do pleno funcionamento do reconhecimento facial realizado no servidor.

- 1.5.1.28. O tratamento de dados pessoais sensíveis por meio de tecnologia de reconhecimento facial deverá ocorrer exclusivamente para fins de segurança patrimonial e institucional, sendo vedada a sua utilização para quaisquer outras finalidades, em conformidade com o art. 11, inciso II, alíneas “a” e “g”, da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais - LGPD).

1.5.2. DETECÇÃO DE PESSOAS COM VOLUMES

- 1.5.2.1. O licenciamento do módulo de detecção de pessoas com volumes deverá ser realizado por câmera (stream de vídeo), considerando exclusivamente as câmeras nas quais o analítico estiver efetivamente habilitado.
- 1.5.2.2. Deverá ser considerada a habilitação do analítico de detecção de pessoas com volumes em 1 (uma) câmera por servidor, totalizando 89 (oitenta e nove) servidores, perfazendo o quantitativo total de 89 (oitenta e nove) licenças de detecção de pessoas com volumes.
- 1.5.2.3. O processamento do analítico de detecção de pessoas com volumes deverá ser realizado localmente, ou seja, exclusivamente no servidor de CFTV da unidade, sem qualquer dependência, total ou parcial, de nuvem externa ou de outros servidores da rede interna.
- 1.5.2.4. O treinamento, reprocessamento ou reindexação dos modelos de IA do analítico de detecção de pessoas com volumes deverá ser realizado em ambiente computacional do CONTRATADO, considerando que os servidores instalados nas unidades não são dimensionados para essa finalidade.
- 1.5.2.5. Deverá permitir o reconhecimento de pessoas portando bolsa, sacola, caixa, mochila ou mala, desde que o objeto apresente altura mínima de 80 (oitenta) pixels e largura mínima de 100 (cem) pixels.
- 1.5.2.6. A detecção deverá ocorrer com pessoas em movimento ou estáticas, de forma individual ou em grupos.
- 1.5.2.7. A detecção deverá ocorrer em objetos com diferentes texturas, cores e dimensões ou parcialmente ocultos.
- 1.5.2.8. A detecção deverá ocorrer em cenários adversos, como alto fluxo de pessoas, objetos de baixa diferenciação visual, iluminação oscilante e pessoas portando múltiplos itens.
- 1.5.2.9. O software deverá minimizar impactos causados por reflexos, sombras intensas e painéis LED piscantes.
- 1.5.2.10. Deverá permitir a configuração de zonas de interesse específicas, tais como entradas, corredores e áreas críticas.
- 1.5.2.11. Deverá permitir a configuração de gravação de pré-evento e pós-evento, de modo a assegurar o registro das imagens e vídeos associados aos alertas gerados.

2. SERVIÇOS DE INSTALAÇÃO

2.1. EQUIPAMENTOS

- 2.1.1. São de responsabilidade do CONTRATADO o fornecimento e a instalação das câmeras IP, bases de fixação, cartões de memória, servidores, switches e demais

acessórios necessários para o funcionamento do sistema de CFTV IP das unidades do BANCO, incluindo o transporte, manuseio e integridade dos materiais, desde a entrega até a aceitação final do BANCO. As estações de monitoramento das unidades e da Central de Segurança do BANCO serão fornecidas pelo BANCO.

- 2.1.2. Todos os componentes fornecidos no escopo da contratação em pauta deverão ser novos, sem uso anterior.
- 2.1.3. É de responsabilidade do CONTRATADO a remoção do sistema de CFTV em uso nas unidades do BANCO.
- 2.1.4. O fornecimento e a instalação dos racks com patch panel nas unidades ficarão a cargo do BANCO.
- 2.1.5. As câmeras IP deverão ser fixadas em alturas e posições definidas no projeto executivo do BANCO.
- 2.1.6. As bases de ligação para acomodação dos cabos e os suportes necessários (hastes, prolongadores, parafusos, buchas, chumbadores, estaiamento com cabo de aço etc.) para fixação das câmeras nos locais indicados deverão ser fornecidos e instalados pelo CONTRATADO.
- 2.1.7. O servidor e o switch de CFTV deverão ser instalados pelo CONTRATADO no rack já existente na agência do BANCO.
- 2.1.8. O CONTRATADO deverá dispor de todos os equipamentos, ferramentas e recursos necessários à execução dos serviços, incluindo equipamentos de proteção individual (EPIS), andaimes, escadas, furadeiras elétricas e demais itens aplicáveis.

2.2. INFRAESTRUTURA

- 2.2.1. O fornecimento e a instalação dos materiais de infraestrutura necessários (eletrodutos, eletrocalhas e cabos) para funcionamento do sistema de CFTV serão de responsabilidade do BANCO.
- 2.2.2. O BANCO disponibilizará o ponto de rede (cabo UTP categoria 6 com path cord de 2 metros e conector RJ-45) no local de instalação de cada câmera e no patch panel do rack.
- 2.2.3. As câmeras deverão ser alimentadas via PoE (Power Over Ethernet), proveniente das portas do switch.
- 2.2.4. O BANCO disponibilizará o ponto elétrico 110 VAC ou 220 VAC (tomada de 10A padrão novo 2P + T), de acordo com a localidade, no rack para instalação do servidor de CFTV.

2.3. SOFTWARES

- 2.3.1. São de responsabilidade do CONTRATADO o fornecimento e a instalação das licenças permanentes do software de CFTV no servidor de gravação, de acordo com a quantidade de câmeras por unidade.
- 2.3.2. O CONTRATADO deverá realizar a instalação e configuração do software de gravação no servidor nas unidades do BANCO relacionadas no **Anexo denominado Plano de Distribuição**.
- 2.3.3. O CONTRATADO deverá realizar a instalação do software de monitoramento na

estação dos usuários nas unidades do BANCO relacionadas no **Anexo** denominado **Plano de Distribuição**.

2.4. FLUXO DE EXECUÇÃO

- 2.4.1. A instalação do sistema de CFTV IP nas unidades deverá ser realizada de acordo com as etapas, prazos e lotes no **Anexo** denominado **Termo de Referência**.
- 2.4.2. A instalação dos equipamentos deverá obedecer ao cronograma fornecido pelo CONTRATADO e aprovado pelo BANCO.
- 2.4.3. Os serviços deverão ser realizados fora do horário de expediente bancário, após às 16h ou o que melhor convir ao BANCO.
- 2.4.4. Caso não haja interferência nas atividades do BANCO, os serviços poderão ser desenvolvidos em horário de expediente.
- 2.4.5. Para execução dos serviços de instalação, configuração e ativação do sistema CFTV IP, bem como a remoção do sistema de CFTV existente, deverão ser adotados os procedimentos dos subitens 2.4.5.1 a 2.4.5.21.
 - 2.4.5.1. Instalar o servidor e o switch no rack já existente na agência;
 - 2.4.5.2. Conectar as fontes de alimentação do servidor e switch nas tomadas do rack, já provenientes da rede de no-break do BANCO;
 - 2.4.5.3. Realizar a configuração dos parâmetros de rede (IP, gateway, máscara) nas câmeras IP, servidor e switch da agência, conforme faixa de endereços disponibilizada pela área de TI do Banco;
 - 2.4.5.4. Instalar a licença permanente do software de CFTV no servidor;
 - 2.4.5.5. Fixar as câmeras IP nos locais indicados no projeto executivo fornecido pelo BANCO.
 - 2.4.5.6. Realizar a conexão das câmeras IP nos pontos de rede já existentes nos locais de instalação;
 - 2.4.5.7. Realizar a conexão das câmeras IP no patch panel do switch;
 - 2.4.5.8. Ajustar o posicionamento e distância focal das câmeras IP, de acordo com o padrão definido pelo BANCO;
 - 2.4.5.9. Realizar a configuração das câmeras IP e software de CFTV, de acordo com padrão definido pelo BANCO;
 - 2.4.5.10. Realizar a instalação do software cliente nas estações de 2 usuários da agência;
 - 2.4.5.11. Realizar o treinamento das funções básicas do software cliente (visualização, reprodução e exportação de imagens) para os usuários da agência;
 - 2.4.5.12. Realizar testes de validação do sistema com a Central de Segurança do BANCO, de acordo com checklist elaborado pelo BANCO;
 - 2.4.5.13. Após a ativação completa do sistema de CFTV IP da agência, realizar a desativação e remoção dos equipamentos do sistema de CFTV existente

(câmeras IP, NVR e switches);

- 2.4.5.14. Realizar registro fotográfico dos equipamentos do sistema de CFTV IP instalado e do sistema de CFTV removido;
- 2.4.5.15. Identificar os equipamentos removidos com fixação de etiqueta;
- 2.4.5.16. Embalar e acondicionar os equipamentos removidos do sistema de CFTV na sala de equipamentos da agência, enquanto se aguarda a destinação da Área de Segurança do BANCO;
- 2.4.5.17. Os discos rígidos (HD) não devem ser formatados, manipulados ou retirados do DVR da agência;
- 2.4.5.18. Realizar a limpeza dos ambientes onde foram prestados os serviços, entregando-os nas mesmas condições encontradas antes do início dos serviços;
- 2.4.5.19. Realizar a correção de eventuais danos em paredes, forros, pisos etc. decorrentes dos serviços de instalação dos equipamentos de CFTV IP ou remoção dos equipamentos existentes de CFTV, de forma a manter o padrão de qualidade e identidade visual das unidades, sem ônus para o BANCO;
- 2.4.5.20. Emitir relatório técnico de instalação, assinado pelo gerente da agência do BANCO, contendo os subitens 2.4.5.21.1 a 2.4.5.21.5.
 - 2.4.5.20.1. Descrição e quantidade de equipamentos instalados, contendo marca, modelo e número de série;
 - 2.4.5.20.2. Certificado da licença do software de CFTV, contendo a quantidade de câmeras suportadas;
 - 2.4.5.20.3. Resultado do checklist dos testes de validação do sistema, conforme item 2.4.5.12;
 - 2.4.5.20.4. Fotografias dos equipamentos do sistema de CFTV instalado e do sistema de CFTV existente removido, conforme item 2.4.5.14;
 - 2.4.5.20.5. Identificação da equipe responsável pela instalação, contendo nome completo, função e número de documento oficial.
- 2.4.5.21. Visando evitar a interrupção da gravação e monitoramento das imagens da agência, o sistema de CFTV existente deverá permanecer em funcionamento até a ativação e validação completa do novo sistema de CFTV.
- 2.4.5.22. A responsabilidade sobre o vazamento de dados e imagens provenientes dos HD, quando não observados os procedimentos descritos neste documento, será imputada exclusivamente ao CONTRATADO.
- 2.4.5.23. O BANCO realizará a fiscalização presencial ou remota da instalação dos equipamentos e softwares de CFTV nas unidades, desde a entrega dos equipamentos até a ativação completa do sistema.

2.5. SERVIÇOS DE DOCUMENTAÇÃO

- 2.5.1. O projeto executivo contendo a localização das câmeras IP e o encaminhamento da

infraestrutura até o rack de rede é de responsabilidade do BANCO.

- 2.5.2. Caso haja alterações em relação ao projeto executivo do item 2.5.1, o CONTRATADO deverá entregar à Área de Segurança do BANCO projeto *as-built* nos formatos DWG (AutoCad) e PDF.

2.6. SERVIÇOS DE TREINAMENTO

- 2.6.1. De acordo com o cronograma aprovado pelo BANCO, o CONTRATADO deverá ministrar treinamento presencial na cidade de Fortaleza/CE para a Área de Segurança do BANCO, conforme os subitens 2.6.1.1 e 2.6.1.2, totalizando 16 (dezesesseis) horas, sem ônus adicional para o BANCO, com os temas dos itens 2.6.1.1 e 2.6.1.2.
- 2.6.1.1. Configuração dos equipamentos e softwares de CFTV IP para a equipe de manutenção do BANCO, com carga horária mínima de 8 (oito) horas;
- 2.6.1.2. Operação do software de CFTV IP para a equipe de monitoramento do BANCO, com carga horária mínima de 8 (oito) horas.

ANEXO I-B**GARANTIA E SERVIÇOS DE ASSISTÊNCIA TÉCNICA****1. GARANTIA**

- 1.1 Todos os equipamentos fornecidos terão garantia contra eventuais defeitos de fabricação pelo período de 36 (trinta e seis meses), contado da emissão do Termo de Aceitação Definitiva (TAD) de cada unidade.
- 1.2 Não estão incluídos na garantia dos produtos as seguintes situações:
 - 1.2.1 defeitos, falhas ou danos ocasionados por vandalismo, assim consideradas aquelas situações nas quais ocorre depredação do equipamento danificando-o no todo ou em parte, ou queda de equipamentos;
 - 1.2.2. defeitos, falhas ou danos ocasionados por trabalhos realizados ou modificações implementadas por pessoal não pertencente ao quadro de empregados do CONTRATADO ou de seus subcontratados;
 - 1.2.3. para as situações descritas nos subitens 1.2.1 e 1.2.2, é necessário que o CONTRATADO apresente relatório técnico comprobatório à Área de Segurança do BANCO.
- 1.3 Todas as outras situações não previstas no item 1.2 deverão ser cobertas pela garantia dos produtos.

2 DESCRIÇÃO DOS SERVIÇOS DE ASSISTÊNCIA TÉCNICA

- 2.1 O CONTRATADO deverá prestar, durante o período de garantia do item 1.1, serviços de assistência técnica para os equipamentos e softwares que compõem o sistema de CFTV IP das agências, compreendendo:
 - 2.1.1. manutenção corretiva on-site dos equipamentos com substituição de peças: serviço destinado a remover eventuais defeitos apresentados pelos equipamentos de CFTV IP, incluindo a substituição de peças, componentes e acessórios, sem qualquer ônus adicional para o BANCO, devendo ser realizada no local de instalação do sistema;
 - 2.1.2. suporte técnico remoto: serviço efetuado via telefone, e-mail ou outro canal de internet, para esclarecimento de dúvidas sobre a utilização do sistema e resolução de problemas de configuração;
 - 2.1.3. atualização de software: serviço para correção de eventuais falhas e vulnerabilidades no software de CFTV, conforme recomendação da área de TI do BANCO ou do fabricante do sistema, podendo ser realizada local ou remotamente;
 - 2.1.4. remanejamento de equipamentos: serviço para mudança do local de instalação dos equipamentos dentro da própria agência ou para outra agência do Banco.
- 2.2 As peças que forem utilizadas na execução dos reparos deverão ser originais, de configuração igual ou superior às substituídas, guardando conformidade com os requisitos do Edital.
- 2.3 Na substituição de algum componente ou periférico este deverá ser compatível com softwares envolvidos, e com as demais partes do equipamento, não podendo ser, em hipótese alguma, de configuração inferior à substituída.

- 2.4 Todo componente, periférico ou acessório diferente do especificado no **Anexo** denominado **Especificações Técnicas** deste Instrumento deverá ser previamente homologado pelo BANCO.
- 2.5 Os serviços de remanejamento de equipamentos poderão ser solicitados por ocasião de alterações de leiaute, mudança de endereço da agência ou quando houver autorização da área de segurança do BANCO. Para fins de estimativa, considerou-se a quantidade de 1 (uma) hora técnica por unidade/mês, totalizando 3.204 (três mil, duzentas e quatro) horas técnicas para 89 unidades ao longo de 36 (trinta e seis) meses.
- 2.6 Para o caso do subitem 2.1.4, deverá ser apresentado orçamento prévio para anuência do BANCO, elaborado em função do número de horas técnicas a serem despendidas na sua execução.
- 2.7 As atualizações do software de CFTV poderão ser realizadas remotamente, de acordo com a autorização da área de TI do BANCO, desde que obedeçam aos requisitos de segurança por meio de VPN (*Virtual Private Network*) ou outro canal de comunicação segura.
- 2.8 No caso de inviabilidade técnica de atualização remota do sistema, o CONTRATADO deverá realizar a atualização *on-site*, sem ônus adicional para o BANCO.

3 ABERTURA E ATENDIMENTO DE CHAMADOS

- 3.1 A abertura de chamados será realizada exclusivamente por unidade administrativa designada pelo BANCO.
- 3.2 O CONTRATADO deverá colocar à disposição do BANCO página na Internet para registro e acompanhamento de chamados.
- 3.3 Em caso de indisponibilidade temporária da página na Internet, deverá ser possível notificar incidentes de falhas ao CONTRATADO via telefone ou correio eletrônico. Os chamados telefônicos notificando incidentes deverão ser atendidos em língua portuguesa pela central de atendimento do CONTRATADO.
- 3.4 O início do tempo de solução de problemas deverá ser contabilizado a partir do registro da ocorrência junto ao CONTRATADO que deverá fornecer um número de identificação do registro. O término do atendimento será caracterizado pelo momento em que o equipamento estiver disponível para uso, em perfeitas condições de funcionamento, conforme aceite do BANCO.
- 3.5 O CONTRATADO deverá disponibilizar, ao longo da vigência do Contrato, mensalmente e até o último dia útil de cada mês, através de página na Internet ou correio eletrônico, planilha(s) eletrônica(s) contendo o detalhamento de informações sobre todos os eventos relativos a atendimentos iniciados e/ou encerrados no período compreendido entre o dia 21 do mês anterior e o dia 20 do mês corrente, para efeito de confrontação com os controles internos do BANCO. A(s) planilha(s) eletrônica(s) referida(s) deverá(ão) conter pelo menos as seguintes colunas:
 - 3.5.1. número do chamado (identificador do chamado no CONTRATADO);
 - 3.5.2. identificador do chamado do BANCO (número de controle do BANCO);
 - 3.5.3. agência Administrativa de atendimento;
 - 3.5.4. número de série do equipamento;
 - 3.5.5. identificação do técnico executor do atendimento;

- 3.5.6. data e hora de abertura do chamado;
 - 3.5.7. data e hora do fechamento do chamado (caso já tenha ocorrido);
 - 3.5.8. descrição sucinta do incidente;
 - 3.5.9. descrição sucinta da solução do incidente (caso já tenha ocorrido);
 - 3.5.10. indicativo se a visita foi improdutiva ou não;
 - 3.5.11. caso nenhum atendimento seja realizado no período, o CONTRATADO deverá sinalizar essa situação para o BANCO através de correio eletrônico.
- 3.6 O CONTRATADO deverá disponibilizar, caso haja solicitação do BANCO, cópias das ordens de serviços referentes aos chamados de assistência técnica, ocorridos até 180 (cento e oitenta) dias antes da solicitação do BANCO, em mídia digital.

4 LOCAL DA PRESTAÇÃO DOS SERVIÇOS

- 4.1 A prestação dos serviços descritos neste Anexo deverá ocorrer nas unidades do BANCO relacionadas no **Anexo** denominado **Plano de Distribuição**, bem como no Ambiente de Segurança Corporativa, localizado em Fortaleza/CE.
- 4.2 O CONTRATADO deverá possuir sede, filial, técnico residente ou empresa subcontratada em cada estado das unidades relacionadas no **Anexo** denominado **Plano de Distribuição** para a prestação dos serviços de assistência técnica durante a vigência contratual.
- 4.3 A seu critério, o BANCO poderá realizar alteração nas unidades relacionadas no **Anexo** denominado **Plano de Distribuição**, comunicando ao CONTRATADO quanto ao novo endereço, para adequação pelo CONTRATADO e ajustes quanto ao prazo de atendimento, se necessário.
- 4.4 Caso os serviços não possam ser executados nas dependências do BANCO, o equipamento avariado poderá ser removido para um Centro de Atendimento Técnico (CAT) do CONTRATADO, mediante justificativa por escrito, relacionando os problemas apresentados, devidamente aceita pelo BANCO e com autorização expressa de saída do equipamento, desde que o equipamento avariado seja substituído por outro equivalente ou de superior configuração.

5 NÍVEIS DE SERVIÇO

- 5.1 O nível de serviço para fins de atendimento dos serviços especificados nos itens 2.1.1 a 2.1.4. deverá considerar os seguintes prazos:
 - 5.1.1. até 24 (vinte e quatro) horas corridas, contado da abertura do chamado pelo BANCO, para as unidades localizadas nas capitais dos estados e respectivas regiões metropolitanas;
 - 5.1.2. até 48 (quarenta e oito) horas corridas, contado da abertura do chamado pelo BANCO, para as demais unidades.
- 5.2 Para efeito de contagem de tempo, caso o chamado seja registrado em finais de semana, feriados nacionais ou em horário fora do expediente bancário, o prazo para atendimento técnico será iniciado a partir das 8h do dia útil seguinte ao da abertura desse chamado;
- 5.3 O atendimento deverá ser realizado independentemente de feriado ou final de semana, salvo disposição em contrário do BANCO;

- 5.4 Para o caso do item 2.3, o reparo e devolução do equipamento não poderá ultrapassar o prazo máximo de 30 (trinta) dias úteis.