ANEXO I-A

ESPECIFICAÇÕES TÉCNICAS DO SISTEMA INTEGRADO DE SEGURANÇA BANCÁRIA

1. SISTEMA INTEGRADO DE SEGURANÇA BANCÁRIA

1.1 Características Gerais do Sistema:

1.1.1 Compreende todos os dispositivos (*hardware* e *software*) componentes de uma plataforma de segurança integrada, envolvendo placas, módulos e circuitos, além de licenças de *software* para gerenciamento, monitoramento e controle centralizado, composta, no mínimo, pelos seguintes subsistemas:

1.1.1.1 Sistema de Alarmes;

1.1.1.2 Sistema de Controle de Acesso;

1.1.1.3 Sistema de Gerador de Neblina;

1.1.1.4 Sistema de CFTV;

1.1.1.5 Sistema de Fechadura com Retardo.

1.1.2 O sistema deverá permitir a operação integrada de todos os subsistemas em uma única plataforma;

1.1.3 Deverão ser fornecidos todos os sistemas e suas licenças dos subitens 1.1.1.1 ao 1.1.1.3, bem como realizar a integração dos sistemas 1.1.1.4 ao 1.1.1.5;

1.1.4 Os quantitativos de equipamentos variam de acordo com as necessidades de cada unidade, conforme **Anexo** denominado **Rede de Unidades**, podendo variar, inclusive zerar, a critério do BANCO em algumas das Unidades;

1.1.5 Todos os equipamentos fornecidos deverão ser compatíveis com a plataforma, garantindo integração nativa e funcionamento pleno conforme especificações técnicas, independentemente de serem novos;

1.1.6 A plataforma do sistema deverá ser cliente-servidor, multiusuário e multissite, com gestão centralizada;

1.1.7 O sistema deverá oferecer suporte aos navegadores Microsoft Edge, Google Chrome e Mozilla Firefox, utilizados em estações de trabalho com sistema operacional Microsoft Windows 11 ou superior, assegurando total compatibilidade com o ambiente computacional do BANCO;

1.1.8 Deverá ter capacidade para suportar, no mínimo, 10.000 (dez mil) usuários;

1.1.9 Deverá possibilitar o cadastro inicial dos usuários a partir de importação do Sistema Pessoal do BANCO;

1.1.10 Deverá possibilitar gerenciar múltiplos sites ou entidades independentes sob uma arquitetura centralizada, mantendo autonomia local e políticas globais (federalização), incluindo:

1.1.10.1 autonomia local;
1.1.10.2 políticas globais sincronizadas;
1.1.10.3 sincronização de eventos e usuários;
1.1.10.4 gerenciamento distribuído;

1.1.10.5 escalabilidade.

1.1.11 Possuir integração com protocolos AD/LDAP e SNMP;

1.1.12 Os operadores de sistema deverão ser integrados ao AD (*Active Directory*) do BANCO;

1.1.13 O sistema deverá ter por idioma padrão em todas as interfaces a língua portuguesa do Brasil;

1.1.14 Deverá ser capaz de lidar com projetos de escalonamento em até o triplo dos componentes do sistema, por meio de expansões modulares ou upgrade de licenças;

1.1.15 Deverá armazenar todas as configurações, logs de auditoria, eventos, alarmes, índice de vídeo e áudio no banco de dados;

1.1.16 O sistema deverá manter auditoria detalhada das operações realizadas, incluindo, no mínimo, logins inválidos, comandos executados, operações de bypass, automações, alterações de configuração e ações efetuadas por operadores que impactam na segurança, tais como arme, desarme, inclusão de usuários e alteração de validade;

1.1.17 Deverá possuir banco de dados robusto com capacidade de armazenar eventos e ações realizadas dos últimos 6 meses, de forma transacional, e dos últimos 24 meses de forma histórica;

1.1.18 O sistema deverá permitir expurgo controlado de eventos, com critérios definidos e registro auditável da operação;

1.1.19 Deverá possuir criptografia de dados em repouso AES-256;

1.1.20 Todas as comunicações cliente-servidor devem se basear no protocolo TCP/ IP padrão;

1.1.21 A plataforma deverá disponibilizar interface WEB nativa, garantindo acesso centralizado às funcionalidades do sistema, complementando clientes desktop quando necessário;

1.1.22 Deverão ser fornecidas, no mínimo, 20 (vinte) licenças de uso simultâneo para as estações da Central de Segurança (clientes);

1.1.23 Deverão ser fornecidas, no mínimo, 2 (duas) licenças de uso simultâneo para as estações de monitoramento (clientes) por Unidade;

1.1.24 Deverá permitir o monitoramento remoto de eventos e alarmes de todos os equipamentos integrados ao sistema na mesma interface;

1.1.25 Deverá permitir ao operador do sistema correlacionar eventos dos subsistemas em interface própria de forma que eventos do sistema de alarme, por exemplo, possa acionar câmeras, liberar portas, acionar gerador de neblina, ou eventos da fechadura de retardo do cofre ou portas acionem o sistema de alarme, câmeras etc.;

1.1.26 O sistema proposto deverá possuir capacidade para emitir alertas sonoros e visuais, sempre que ocorrer falha de comunicação ou interrupção da alimentação elétrica (AC) nos subsistemas (1.1.1.1 a 1.1.1.5);

1.1.27 A interface deverá possuir filas de atendimento, com nomes e quantidades configuráveis;

1.1.28 Deve permitir criar orientações e descrições para cada tipo de evento;

1.1.29 O sistema deverá permitir associar instruções operacionais e orientações específicas a cada tipo de evento, exibidas automaticamente ao operador no momento do atendimento;

1.1.30 Deve permitir que o usuário faça o registro de atendimento de um evento de alarme;

1.1.31 Deverá permitir o registro do tempo de atendimento de cada etapa do fluxo de operação, passíveis de relatórios e auditoria executadas pelo próprio sistema;

1.1.32 Deverá permitir o emprego de fluxo pré-definido de procedimentos, por meio de interface para a configuração destes fluxos, os quais deverão ser vinculados ao tipo de evento em tratamento;

1.1.33 O fluxo deverá ser configurável por tipo de atendimento, além de possuir auditoria completa do processo de criação e preenchimento;

1.1.34 A comunicação do software com os dispositivos componentes do sistema integrado deverá ser em tempo real, utilizando a rede corporativa do BANCO;

1.1.35 Os subsistemas deverão se comunicar com interface ethernet nativa, sem utilização de conversores externos;

1.1.36 Deverá permitir a geração e exportação de relatórios com parâmetros a seguir relacionados, sem a necessidade de desenvolvimento, em nível de código de sistema, incluindo filtros e ordenação de informações, recebidas ou geradas pelo sistema e armazenadas em seu banco de dados:

1.1.36.1 Data e hora;
1.1.36.2 UF;
1.1.36.3 Cidade;
1.1.36.4 Unidade;
1.1.36.5 Sistema (conforme relação do item 1.1.1);
1.1.36.6 Equipamento do Sistema;
1.1.36.7 Usuário;
1.1.36.8 Evento;
1.1.36.9 Informação complementar do evento, se houver.

1.1.37 Deverá possuir recurso de restauração de configuração, de maneira que não seja necessário em caso de perda de configuração do sistema refazer novos cadastramentos ou reconfigurações;

1.1.38 Deverá permitir o cadastro de operadores com níveis distintos de privilégios;

1.1.39 O sistema integrado deverá possibilitar o cadastramento e o monitoramento ilimitado de todos os equipamentos vinculados aos subsistemas (1.1.1.1 a 1.1.1.5), sem qualquer restrição quanto à quantidade de dispositivos gerenciados, assegurando plena escalabilidade e gestão centralizada, em conformidade com a arquitetura integrada;

1.1.40 Deverá permitir o envio automático de e-mail ou demais tipos de alertas para notificação de eventos e alarmes;

1.1.41 Deverá disponibilizar APIs devidamente documentadas, podendo incluir SDK quando aplicável, para integração com outros sistemas corporativos;

1.1.42 Deverá estar em conformidade com a LGPD, ao que couber proteção de dados de usuários dos sistemas;

1.1.43 Deverá possibilitar uma interface mobile com perfil de acesso a ser customizado para o gestor da unidade.

1.2 Características Específicas para o Sistema de Alarme:

Conforme o **Anexo** denominado **Especificações Técnicas do Sistema de Alarme**.

1.3 Características Específicas para o Sistema de Controle de Acesso Físico:

Conforme o **Anexo** denominado **Especificações Técnicas do Sistema de Controle de Acesso Físico**.

1.4 Características Específicas para o Sistema de Gerador de Neblina:

Conforme o **Anexo** denominado **Especificações Técnicas do Sistema de Gerador de Neblina**.

1.5 Características Específicas para CFTV:

1.5.1 Deverá integrar o sistema SecurOS® VMS, da Empresa ISS, implantado do BANCO, possibilitando:

1.5.1.1 visualização instantânea;

1.5.1.2 visualização de reprodução de gravação;

1.5.1.3 visualização de múltiplas câmeras de vários servidores, em diversas e distintas localidades em uma interface única;

1.5.1.4 a utilização do recurso de zoom digital em imagens;

1.5.1.5 controle de imagem geradas por câmeras *fisheyes*;

1.5.1.6 vincular eventos do sistema integrado às câmeras ou trechos de vídeo do sistema de CFTV;

1.5.1.7 processar integração de eventos dos analíticos de vídeos;

1.5.1.8 gerar alarme quando da ocorrência de falha de funcionamento da câmera IP;

1.5.1.9 monitorar parâmetros dos recursos do CFTV via SNMP ou protocolo com funcionalidade similar;

1.5.1.10 acionamento de saídas de alarme das câmeras IP, caso possuam;

1.5.1.11 inserir mapa sinóptico para visualização e acesso às câmeras do sistema.

1.6 Características Específicas para Dispositivo de Fechamento com Retardo Randômico:

1.6.1 Deverá integrar o sistema SOFTWARE SGS INTERGARD®, da InterGard do Brasil LTDA, implantado do BANCO;

1.6.2 Deverá possuir a função integrada de gerar senhas dinâmicas para ativação do retardo da fechadura cadastrada e específica de cada cofre;

1.6.3 Deverá possuir função de bloqueio remoto imediato do cofre;

1.6.4 Deverá permitir o monitoramento de status do dispositivo, como: porta aberta/fechada, ferrolho aberto/fechado, violações, portas abertas por tempo superior ao limite programado e demais alertas nativos do dispositivo.

ANEXO I-B

ESPECIFICAÇÕES TÉCNICAS DO SISTEMA DE ALARME

1. CARACTERÍSTICAS ESPECÍFICAS PARA O SISTEMA DE ALARME

1.1 Deverá ser assegurada a integração do sistema com as plataformas de operação e gestão, por meio da utilização de protocolos padrão SIA, Contact ID ou *APIs* abertas;

1.2 Deve possibilitar a utilização de criptografia de ponta a ponta na comunicação entre a central, o software e os dispositivos, por meio de protocolos seguros de comunicação, tais como TLS/SSL, ou tecnologias equivalentes de criptografia robusta (por exemplo, AES ou similares), garantindo a proteção, integridade e confidencialidade dos dados transmitidos.

1.3 Deverá possibilitar a extração de relatórios (HTML/PDF/RTF/XLS/TXT) abrangendo eventos de alarme, configurações de zoneamento, registros de auditoria e permissões atribuídas aos operadores, contemplando um período mínimo de 365 dias;

1.4 Deve possuir configuração de prioridade de ocorrências;

1.5 Deve permitir Upload/Download completo configurações aplicadas ao módulo de controle;

1.6 Deve permitir atualização de *firmware* via rede ethernet (TCP/IP);

1.7 Deve permitir o ajuste de parâmetros para ativação/desativação da central ou de seus periféricos de forma remota;

1.8 Deve permitir a configuração remota dos parâmetros que couberem dos periféricos do sistema de alarme;

1.9 Deve permitir o *bypass* de zonas;

1.10 Deve permitir o gerenciamento remoto dos de usuários ou grupo de usuários;

1.11 Deve permitir a configuração dos módulos de controle por lote;

1.12 Deverá possibilitar a criação de padrões (templates) reutilizáveis aplicados para comportamentos de partições, teclados e sensores. A criação, edição e exclusão destes padrões devem passar por regras de permissionamento;

1.13 Deve permitir o diagnóstico remoto do conjunto de hardware instalado na agência;

1.14 Deve permitir o monitoramento remoto do status do sistema instalado na agência;

1.15 Deve oferecer suporte à automação de rotinas, incluindo a execução de testes automáticos, agendamento de tarefas;

1.16 Deverá permitir configurar feedbacks sonoros, audíveis junto nos equipamentos de identificação, sendo, no mínimo, atraso de arme, atraso de desarme, alarme, porta aberta muito tempo;

1.17 Deverá permitir, de forma configurável, restringir o acesso de usuários até que um usuário master realize o primeiro acesso, com possibilidade de definição de janelas horárias.

2. EQUIPAMENTOS DO SISTEMA DE ALARME

2.1. CENTRAL - Modulo de controle

2.1.1 A central de alarme deverá ser constituída por equipamento dedicado à função de segurança eletrônica, com hardware e firmware próprios do fabricante, não sendo aceitas implementações baseadas em plataformas de prototipagem ou computadores de propósito geral;

2.1.2 Deverá monitorar todas as funções dos sensores periféricos do alarme;

2.1.3 Deverá ter função de programar todas as funções do alarme, locais e remotas;

2.1.4 Deverá possuir, no mínimo, 8 (oito) partições;

2.1.5 O sistema deverá possuir capacidade modular que permita expansões, contemplando, no mínimo, 99 (noventa e nove) zonas híbridas, integrando conexões cabeadas e sem fio;

2.1.6 Deverá permitir a identificação dos periféricos conectados via barramento (*BUS*) e sem fio, por meio de endereçamento lógico;

2.1.7 Permitir programação da ativação automática da proteção noturna para cada partição (arme automático), em horário a ser definido pelo BANCO;

2.1.8 Possuir recurso de supervisão de todos os componentes interligados;

2.1.9 Permitir parametrização da solução de hardware através de interface de sistema ou teclado;

2.1.10 As parametrizações citadas acima compreendem, no mínimo:

2.1.10.1 ativar e desativar partições;
2.1.10.2 bloquear e desbloquear zonas;
2.1.10.3 habilitar modo teste.

2.1.11 Permitir a ligação de mais de um teclado de operação;

2.1.12 Possibilitar a configuração de retardo de zona sem disparar as sirenes, bem como o tempo para restauração automática deste retardo após a ocorrência da intrusão;

2.1.13 Possibilitar a programação de tempo de disparo das sirenes;

2.1.14 Possuir detecção de *tamper* (violação física);

2.1.15 Deverá enviar todos os eventos de alarme pelas vias de comunicação, no mínimo:

2.1.15.1 rede ethernet (TCP/IP) corporativa do BANCO: principal;
2.1.15.2 telefonia móvel (no mínimo 4G): contingência.

2.1.16 O envio de eventos baseados em comunicação ethernet e telefonia móvel com transporte e controle de alarmes de alta velocidade deverão possuir protocolos de segurança com criptografia no mínimo AES 256 bits;

2.1.17 Todas as vias deverão ter recurso de supervisão de disponibilidade, reportando à Central de Monitoramento com as seguintes periodicidades:

2.1.17.1 rede ethernet (TCP/IP) corporativa do BANCO: 10 (dez) minutos;
2.1.17.2 telefonia móvel (no mínimo 4G): 30 (trinta) minutos.

2.1.18 Deverá enviar, no mínimo, os seguintes tipos de ocorrências:

2.1.18.1 Ativação/desativação da Central ou suas partições, independentemente do horário em que elas ocorrerem;

2.1.18.2 Ingresso fora do horário autorizado, inclusive em finais de semana e feriados;

2.1.18.3 Ingresso com senha de pânico;

2.1.18.4 Desativação total ou parcial da Central de Alarme, fora do horário autorizado, inclusive em finais de semana e feriados;

2.1.18.5 Detecção de presença;

2.1.18.6 Detecção de fumaça;

2.1.18.7 Detecção de impacto;

2.1.18.8 Detecção de abertura magnética;

2.1.18.9 Detecção de quebra de vidro;

2.1.18.10 Acionamento por botão de pânico;

2.1.18.11 Violação de sensores e receptores;

2.1.18.12 Sensor ou acionador de pânico, com defeito ou bateria fraca;

2.1.18.13 Sirene violada ou desligada;

2.1.18.14 Falta de alimentação pela rede pública de energia elétrica;

2.1.18.15 Conexão e desconexão de bateria;

2.1.18.16 Falha de comunicação de alguma via de transmissão;

2.1.18.17 Desativação e não ativação do arme automático;

2.1.18.18 Supervisão das vias de comunicação e periféricos;

2.1.19 Deverá executar o comando de arme/desarme remoto pelo operador da central de monitoramento;

2.1.20 Deverá possibilitar a emissão de alertas nos modos ‘teste’ ou ‘manutenção’, garantindo que não haja acionamentos desnecessários pela central de monitoramento;

2.1.21 Deve permitir teste nos sensores em tempo real a qualquer momento, mesmo com a central desarmada;

2.1.22 Deverá, mesmo com o sistema desarmado, a central de alarme deve manter a recepção de todos os eventos dos sensores, com o objetivo de assegurar a rastreabilidade e a auditoria do funcionamento integral dos equipamentos;

2.1.23 Deve permitir configurar tempo para ignorar falso evento de intrusão;

2.1.24 Deve permitir arme automático por agendamento de horário distinto por dias da semana;

2.1.25 Deve possibilitar quando da indisponibilidade de rede que todas as regras de negócios locais continuem em funcionamento, sem interferir nas regras de negócios específicas para quando o equipamento estiver sem comunicação com o servidor;

2.1.26 Deve permitir a configuração de zonas individualmente;

2.1.27 Deverá permitir a configuração individual dos sensores a qual partição pertence, sem limite de sensores por partição.

2.2. RECEPTORA

2.2.1 Deverá ser compatível com o item 2.1 (CENTRAL);
2.2.2 Deve possuir conexão via BUS com a central;
2.2.3 Deve possibilitar comunicação sem fio com dispositivos compatíveis;
2.2.4 Deverá possuir capacidade de endereçamento lógico;
2.2.5 Deverá suportar comunicação unidirecional e bidirecional;
2.2.6 Deverá permitir a supervisão dos dispositivos sem fio;
2.2.7 Deve permitir integração com múltiplos dispositivos sem fio (sensores, controle remoto, sirenes);
2.2.8 Deve possuir detecção de *tamper* (violação física);
2.2.9 Deve possuir Monitoramento de sinal;
2.2.10 Deve possuir alerta de *jamming* (interferência);
2.2.11 Deve possuir indicador de qualidade de RF;
2.2.12 Deve permitir a integração com software de configuração.

2.3. SENSOR DE PRESENÇA INTERNO TIPO I

2.3.1 Deverá ser compatível com os itens 2.1 (CENTRAL);
2.3.2 Deverá dispor de comunicação unidirecional ou bidirecional;
2.3.3 Deverá possuir tecnologia de detecção por infravermelho e micro-ondas integradas;
2.3.4 Deverá ter cobertura de no mínimo 12m de raio por 85º;
2.3.5 Deverá ter tecnologia antimascaramento com utilização de produto líquido, viscoso ou em pó de forma borrifada ou espalhada por pincel, isopor, papelão, manta térmica, guarda-chuva, madeira, acrílico ou outros materiais;
2.3.6 Deverá ter recurso de compensação de temperatura, para o infravermelho;
2.3.7 Deverá ter recurso de ajuste de limite de detecção do micro-ondas;
2.3.8 Deverá ter recurso de *tamper* da tampa e da parede;
2.3.9 Deverá possuir Imunidade a correntes de ar, insetos e pequenos animais, de forma a minimizar falsos positivos;
2.3.10 Deverá possuir recurso de teste e supervisão;
2.3.11 Deverá possuir tecnologia de detecção de disfarces e camuflagens;
2.3.12 Deverá possuir ao menos uma das certificações e aprovações como: CE, WEEE, FCC, GOST, UL ou equivalentes nacionais;
2.3.13 Deverá possuir *LEDs* indicadores de alarmes e funções;
2.3.14 Deverá possuir grau de proteção, no mínimo, IP30, IK04;
2.3.15 Possuir proteção contra disparos falsos causados por luz branca.

2.4. SENSOR DE PRESENÇA INTERNO TIPO II

2.4.1 Deverá ser compatível com os itens 2.1 (CENTRAL);
2.4.2 Deverá dispor de comunicação unidirecional ou bidirecional;
2.4.3 Deverá possuir tecnologia de detecção por infravermelho e micro-ondas integradas;
2.4.4 Deverá ter cobertura de no mínimo 5m de raio por 360º;
2.4.5 Deverá ter recurso de ajuste de sensibilidade;
2.4.6 Deverá ter recurso de *tamper*;
2.4.7 Deverá possuir recurso de teste e supervisão;
2.4.8 Deverá possuir ao menos uma das certificações e aprovações como: CE, WEEE, FCC, GOST, UL ou equivalentes nacionais;

2.4.9 Deverá possuir LEDs indicadores de alarmes e funções.

2.5. SENSOR DE PRESENÇA EXTERNO

2.5.1 Deverá ser compatível com os itens 2.1 (CENTRAL);
2.5.2 Deverá dispor de conexão física, por meio de cabeamento;
2.5.3 Deverá dispor de comunicação unidirecional ou bidirecional;
2.5.4 Deverá ter do tipo para uso externo, com proteção a incidência solar e chuvas;
2.5.5 Deverá possuir tecnologia de detecção por infravermelho e micro-ondas integradas;
2.5.6 Deverá ter cobertura de no mínimo 10m;
2.5.7 Deverá ter recurso de compensação de temperatura, para o infravermelho;
2.5.8 Deverá ter recurso de ajuste de sensibilidade;
2.5.9 Deverá ter recurso de *tamper*;
2.5.10 Deverá possuir Imunidade a correntes de ar, insetos e pequenos animais, de forma a minimizar falsos positivos;
2.5.11 Deverá possuir recurso de teste e supervisão;
2.5.12 Deverá possuir ao menos uma das certificações e aprovações como: CE, WEEE, FCC, GOST, UL ou equivalentes nacionais;
2.5.13 Deverá possuir LEDs indicadores de alarmes e funções;
2.5.14 Deverá possuir grau de proteção, no mínimo, IP 54.

2.6. SENSOR DE FUMAÇA

2.6.1 Deverá ser compatível com os itens 2.1 (CENTRAL);
2.6.2 Deverá dispor de conexão física, por meio de cabeamento;
2.6.3 Deverá possuir tecnologia de detecção por sensor ótico e sensor térmico;
2.6.4 Deverá ter cobertura de área de no mínimo 20m²;
2.6.5 Deverá ter recurso de *tamper*;
2.6.6 Deverá possuir recurso de autoteste e supervisão;
2.6.7 Deverá possuir ao menos uma das certificações e aprovações como: CE, WEEE, FCC, GOST, UL ou equivalentes nacionais;
2.6.8 Deverá possuir LEDs indicadores de alarmes e funções.

2.7. SENSOR DE CHOQUE/IMPACTO

2.7.1 Deverá ser compatível com o item 2.1 (CENTRAL);
2.7.2 Deverá dispor de conexão física, por meio de cabeamento;
2.7.3 Deverá atuar na detecção de vibrações, choques, impactos, perfurações, cortes, escavações, rompimentos ou ataques mecânicos contra paredes, divisórias, compartimentos protegidos ou estruturas equivalentes, permitindo ajuste de sensibilidade conforme o material monitorado;
2.7.4 Deverá possuir discriminação configurável entre vibrações ambientais normais e eventos de ataque, visando reduzir alarmes falsos;
2.7.5 Deverá ter recurso de *tamper*;
2.7.6 Deverá possuir recurso de teste, aprendizagem e supervisão;
2.7.7 Deverá possuir ao menos uma das certificações e aprovações como: CPR, CE, GOST, UL ou equivalente nacionais;
2.7.8 Deverá possuir *LEDs* indicadores de alarmes e funções.

2.8. SENSOR DE ABERTURA MAGNÉTICO

2.8.1 Deverá ser compatível com os itens 2.1 (CENTRAL);
2.8.2 Deverá dispor de conexão física, por meio de cabeamento;
2.8.3 Deverá dispor de comunicação unidirecional ou bidirecional;
2.8.4 Deverá permitir a supervisão periódica.

2.9. SENSOR QUEBRA VIDRO

2.9.1 Deverá ser compatível com os itens 2.1 (CENTRAL);

2.9.2 Deverá dispor de conexão física, por meio de cabeamento;
2.9.3 Deverá reconhecer quebra de vidro plano, temperado, laminado e aramado;
2.9.4 Deverá ter sensibilidade ajustável;
2.9.5 Deverá ter recurso de *tamper*;
2.9.6 Deverá ter um alcance mínimo de 6m;
2.9.7 Deverá permitir a instalação no teto ou parede;
2.9.8 Deverá possuir recurso de teste, aprendizagem e supervisão;
2.9.9 Deverá possuir a tecnologia de detectação de quebra de vidro com análise digital por reconhecimento de padrões (multi-faixa);
2.9.10 Deverá possuir ao menos uma das certificações e aprovações como: CPR, CE, GOST, UL ou equivalente nacionais;
2.9.11 Deverá possuir LEDs indicadores de alarmes e funções;

2.10. TECLADO DE OPERAÇÕES DO ALARME

2.10.1 Deverá ser compatível com o item 2.1 (CENTRAL);
2.10.2 Deverá possuir teclas numéricas e especiais de funções de navegação e controle do sistema de alarme;
2.10.3 Deverá possuir *display* de exibição de informações/mensagens em português do sistema de alarme;
2.10.4 Deverá possuir indicações visuais e/ou sonoras a respeito de *status* do sistema de alarme e funcionamento do mesmo, como armado, desarmado e eventuais problemas;
2.10.5 Deverá possuir capacidade de acesso a todas as zonas;
2.10.6 Deverá possuir função de alertas por violação (*tamper*).

2.11. ACIONADOR REMOTO DE PÂNICO

2.11.1 Deverá ser compatível com os itens 2.1 (CENTRAL) e 2.2 (RECEPTORA);
2.11.2 Deverá dispor de conexão sem fio;
2.11.3 Deverá possuir capacidade de endereçamento lógico;
2.11.4 Deverá dispor de comunicação unidirecional ou bidirecional;
2.11.5 Deverá ser do tipo acionador portátil de alarme tipo controle remoto sem fio;
2.11.6 Deverá ter código único para cada acionador permitindo a identificação do usuário;
2.11.7 Deverá acionar o sistema de alarme de maneira silenciosa e discreta, de qualquer local no interior da Unidade do BANCO, sendo alimentado através de baterias internas;
2.11.8 Deverá possuir recurso de monitoramento ativo dos acionadores remotos de pânico (keep alive), com verificação periódica da comunicação, reporte do nível de bateria e geração de evento técnico em caso de ausência de resposta;
2.11.9 Deverá possuir recurso para evitar o acionamento involuntário (antiacidental);
2.11.10 Deverá funcionar em qualquer local da Unidade. Portanto, deverão ser instalados tantos receptores e/ou repetidores quantos forem necessários para prover cobertura ao seu adequado funcionamento;
2.11.11 Deverá ser necessário acionar apenas 1 botão para ativação do alarme (caso o acionador tenha mais de um botão);
2.11.12 Deverá possuir ao menos uma das certificações e aprovações como: CE, WEEE, FCC, GOST, UL, ou equivalentes nacionais, como Anatel.

2.12. SIRENE AUTOALIMENTADA

2.12.1 Deverá ser compatível com o item 2.1 (CENTRAL);
2.12.2 Deverá dispor de conexão física, por meio de cabeamento;
2.12.3 Deverá ser do tipo autoalimentada com bateria interna recarregável, com duração de aproximadamente 15 minutos em plena potência;
2.12.4 Deverá possuir alimentação própria para o caso de violação dos fios de alimentação;
2.12.5 A sirene instalada no ambiente externo deverá ter caixa de proteção, resistente a vandalismos;
2.12.6 Deverá ter recurso de *tamper*;
2.12.7 A caixa da sirene externa deverá possuir chave com fechadura para desativação em caso de corte ou manutenção;

2.12.8 Deverá ter capacidade de configuração de tempos de disparo;
2.12.9 Deverá ter Potência acústica mínima de 100 dB a 1 metro.

ANEXO I-C

ESPECIFICAÇÕES TÉCNICAS DO SISTEMA DE CONTROLE DE ACESSO FÍSICO

1. CARACTERÍSTICAS ESPECÍFICAS DO SISTEMA DE CONTROLE DE ACESSO FÍSICO

1.1 O Sistema de Controle de Acesso Físico (SCAF) deverá prover controle, monitoramento, auditoria e gestão de acessos físicos às dependências do Banco do Nordeste, com foco em segurança, disponibilidade, rastreabilidade, integração corporativa e escalabilidade;

1.2 Deverá permitir implementação de regras de acesso, como:

1.2.1 Intertravamento;
1.2.2 Anti-passback;
1.2.3 Custódia simples e dupla (um ou dois usuários autenticados para o acesso);
1.2.4 Regras por usuário, perfil ou equipamento;
1.2.5 Programação por horário, dia e data;
1.2.6 Situações de coação;

1.2 Deverá permitir a indicação de atendimento da requisição de abertura por parte da Central de Monitoramento do Banco do Nordeste;

1.3 Deverá exibir na tela de monitoramento de eventos as solicitações de acesso gerados com biometria;

1.4 Deverá receber evento de solicitação de abertura remota e assistida, contendo na mesma tela os dados de identificação do usuário e a visualização em tempo real da câmera local;

1.6 A liberação da porta deverá ser realizada através de comando disponível na mesma tela de monitoramento de eventos;

1.7 Deverá gerar alarme sonoro e visual à Central de Monitoramento, como:

1.7.1 porta aberta/fechada;
1.7.2 acionamento das botoeiras;
1.7.3 violações nos componentes;
1.7.4 porta aberta por tempo superior ao limite programado;
1.7.5 demais alertas nativos dos componentes.

1.8 Deverá controlar, no mínimo, 5 (cinco) pontos de acesso de cada unidade do BANCO com seus respectivos acessórios (leitores, fechaduras, acionadores e botoeiras);

1.9 O sistema deverá dispor de software de controle de acesso com arquitetura moderna, escalável e segura, atendendo aos seguintes requisitos:

1.9.1 Arquitetura modular;
1.9.2 Capacidade de operação multissite, com gestão centralizada de múltiplas unidades;
1.9.3 Interface web ou cliente dedicado, com perfis administrativos hierarquizados;
1.9.4 Dashboards operacionais e gerenciais, contendo métricas como:

1.9.4.1 Acessos permitidos e negados;
1.9.4.2 Alarmes ativos;
1.9.4.3 Tempo de atendimento das solicitações.

1.9.5 O sistema deverá permitir a geração de relatórios parametrizáveis e exportáveis, com possibilidade de filtragem por período, unidade, usuário, credencial, ponto de acesso e tipo de evento. Os relatórios deverão observar, no mínimo, a seguinte estrutura padrão:

1.9.5.1 Identificação do relatório (título, data e hora de geração);
1.9.5.2 Período de referência das informações;
1.9.5.3 Identificação da unidade, local ou ponto de acesso;
1.9.5.4 Identificação do usuário, visitante ou credencial, quando aplicável;
1.9.5.5 Tipo de evento (acesso autorizado, acesso negado, tentativa de acesso, entre outros);
1.9.5.6 Data e hora do evento;
1.9.5.7 Status do evento e eventual justificativa;
1.9.5.8 Identificação do usuário ou sistema responsável pelo registro, quando aplicável.

1.9.6 Os relatórios deverão ser exportáveis, obrigatoriamente, nos formatos PDF, CSV e XLSX, de modo a possibilitar análise, auditoria, tratamento de dados e integração com sistemas corporativos da Administração, devendo ainda permitir verificação de integridade e rastreabilidade, assegurando a confiabilidade, a autenticidade e a não alteração das informações;

1.9.7 Todo o tráfego de dados deverá ser criptografado;

1.9.8 O sistema deverá permitir auditoria completa de acessos, eventos e ações administrativas;

1.9.9 O sistema deverá respeitar princípios de segregação de funções e perfis de acesso.

1.10 O sistema deverá permitir integração nativa com AD/LDAP para importação e sincronização de usuários, operadores, credenciais e grupos;

1.11 O sistema deverá permitir importação em lote e atualização programada de usuários e credenciais por tarefas agendadas;

1.12 O sistema deverá permitir configuração de níveis de ameaça com execução automática de ações sobre portas, áreas, privilégios e alarmes;

1.13 O sistema deverá permitir operação e monitoramento de portas e leitores em mapas gráficos interativos;

1.14 O sistema deverá permitir correlação entre eventos de acesso e vídeo associado;

1.15 Deverá assegurar integração plena com sistemas corporativos existentes ou futuros, atendendo aos seguintes critérios:

1.15.1 Disponibilização de APIs documentadas, podendo incluir SDK, quando aplicável, com documentação técnica suficiente para permitir integrações e desenvolvimento por terceiros autorizados;

1.15.2 Autenticação por mecanismos seguros;

1.15.3 Suporte à integração com:

1.15.3.1 Sistemas de identidade (IAM/AD);
1.15.3.2 Sistemas de vídeo (VMS);
1.15.3.3 Plataformas de monitoramento e SIEM.

1.15.4 Exportação de eventos em formatos estruturados.

2. EQUIPAMENTOS DE CONTROLE DE ACESSO FÍSICO

2.1. MÓDULO DE CONTROLE DE ACESSO

2.1.1. Deverá ser acompanhado de licença para conexão ao software fornecido de controle de acesso, conforme item 1.

2.1.2. Deverá interligar-se ao servidor de controle de acesso através do padrão Ethernet, sob o protocolo TCP/IP, com velocidade mínima de 100 Mbps, via par trançado, utilizando a rede corporativa do BNB;

2.1.3. Os módulos de controle de acesso deverão possuir interface Ethernet on-board (nativa). Sistemas utilizando conversores ou dispositivos externos anexados para transferência de dados em modo serial através de rede TCP/IP não serão aceitos;

2.1.4. Deverá possuir arquitetura embarcada dedicada para controle de acesso, incluindo armazenamento de firmware, credenciais, regras de acesso e registros operacionais em componentes eletrônicos próprios e integrados ao equipamento, não sendo aceitas soluções cujo funcionamento principal dependa exclusivamente de plataformas de prototipagem ou computadores de propósito geral;

2.1.5. Deverá possuir interfaces para as interconexões dos periféricos (leitora, fechadura, acionadores, botoeiras etc.);

2.1.6. Deverá suportar as leitoras especificadas neste documento;

2.1.7. Deverão ser fornecidas fontes de alimentação e baterias para os módulos de controle de acesso, com autonomia mínima de funcionamento de 2 (duas) horas contínuas;

2.1.8. A fonte de alimentação deverá ser automática, de 100 a 240VAC, 60Hz, com proteção contra curto-circuito, sobreaquecimento e surto de tensão;

2.1.9. Deverá dispor de memória suficiente para armazenar os dados de, no mínimo, 100.000 (cem mil) registros de acessos;

2.1.10. Deverá desempenhar as funções de controle de acesso mesmo quando houver perda de comunicação com o servidor (modo de operação off-line);

2.1.11. No modo de operação off-line, deverão ser validados, no mínimo, a biometria facial, a área de acesso, o prazo de expiração do acesso e a faixa horária permitida;

2.1.12. Após a atualização da base de dados interna do controlador de acesso, cada módulo deverá estar apto para trabalhar em modo off-line, tendo em vista que na ocorrência de indisponibilidade do servidor, os módulos deverão continuar funcionando normalmente, de forma independente, executando as rotinas de validação previstas;

2.1.13. O módulo de controle de acesso deverá armazenar os eventos, durante o período no qual ele permaneceu off-line, para transferi-los ao servidor, de forma automática, tão logo seja restabelecida a rede de comunicação;

2.1.14. Deverá possuir mecanismo que garanta o armazenamento dos dados do relógio interno.

2.2. LEITOR BIOMÉTRICO FACIAL

2.2.1. Deverá realizar autenticação por reconhecimento facial, com detecção de vivacidade para evitar fraudes;

2.2.2. Deverá possuir display no máximo de 7” (polegadas);

2.2.3. Deverá possuir dimensão horizontal (base) de no máximo de 5” (polegadas) de largura, dada peculiaridades dos locais de instalação, incluindo perfilados metálicos;

2.2.4. Capacidade de identificação rápida (tempo de resposta máxima de 1 segundo) em ambientes internos e externos;

2.2.5. Suporte ao protocolo OSDP v2 Secure Channel (SC) ou protocolo proprietário equivalente com comunicação criptografada bidirecional entre leitora e controlador;

2.2.6. Deve possuir duas ou mais câmeras de resolução mínima de 2MP;

2.2.7. Deve possuir iluminação infravermelho integrada;

2.2.8. Capacidade de armazenamento local para mínimo de 10.000 templates faciais;

2.2.9. Deve possuir as interfaces de comunicação RS-485, entrada/saída Wiegand e Ethernet;

2.2.10. Deve possuir a alimentação PoE ou 12Vdc;

2.2.11. Deve possuir os protocolos de rede TCP/IP, com suporte a TLS1.2 ou criptografia AES-256;

2.2.12. Deve possuir indicadores visuais e sonoros para feedback ao usuário durante a autenticação;

2.2.13. Grau de proteção mínimo IP65 contra poeira e água;

2.2.14. A leitora que for fornecida para uso em ambiente externo, deverá ser provida de housing antivandalismo resistente, fixado adequadamente, conforme modelo, de forma a dificultar furtos e ataques, além de seu acrílico ou vidro, então a frente do usuário deve ser do tipo antirreflexivo e compatível com os sensores óticos utilizados pela leitora fornecida forma a não prejudicar o seu funcionamento;

2.2.15. Deverá possuir compatibilidade com sistemas de controle de acesso e integração com os itens especificados neste documento.

2.3. FECHADURA ELETROMECÂNICA

2.3.1. Deverá permanecer travada na ausência de energia elétrica (fail secure);

2.3.2. Deverá permitir abertura manual por dispositivo próprio mecânico, em caso de falha elétrica;

2.3.3. Deverá possuir saída NO/NC para indicar estado;

2.3.4. Deverá possuir força de retenção mínima superior a 500 kgf;

2.3.5. Deverá ser compatível com portas de vidro, madeira (maciça ou compensada) ou folha metálica;

2.3.6. Poderá ser utilizada estruturas metálicas para adaptação das fechaduras às peculiaridades das portas, que deverão ser providas pela Empresa contratada;

2.3.7. Possuir certificações válidas: CE, RoHS ou equivalentes, garantindo conformidade com normas aplicáveis;

2.3.8. Deverá possuir acabamento e resistência com corpo em aço inoxidável ou liga metálica anticorrosiva, adequado para uso interno/externo;

2.3.9. Deverá possuir compatibilidade com sistemas de controle de acesso e integração com os itens especificados neste documento.

2.4. BOTOEIRA DE SAÍDA

2.4.1. Acionamento por botão pulsador com retorno automático;

2.4.2. Deve permitir integração com sistemas de controle de acesso e dispositivos de travamento eletromecânico;

2.4.3. Construção em material metálico resistente (ex.: aço inox ou equivalente), garantindo durabilidade e resistência a vandalismo;

2.4.4. Deve permitir instalação compatível com batentes, paredes ou caixas padrão elétrica, permitindo fixação embutida ou sobreposta;

2.4.5. Deve possuir sinalização visual (ex.: LED) ou indicação clara de acionamento, quando aplicável;

2.4.6. Deve atender às normas de segurança aplicáveis para dispositivos de acionamento em sistemas de controle de acesso.

2.5. ACIONADOR TIPO CHAVE LIGA/DESLIGA

2.5.1. Deverá possuir acionamento manual por chave com posições fixas (ON/OFF);

2.5.2. Indicado para controle permanente de dispositivos ou bloqueio de sistemas;

2.5.3. Deve possuir cilindro metálico de alta durabilidade;

2.5.4. Placa frontal metálica com acabamento resistente à corrosão;

2.5.5. Compatível com sistemas de controle de acesso e travas eletromecânicas;

2.5.6. Instalação embutida ou sobreposta em batentes ou caixas padrão elétrica;

2.5.7. Sinalização visual (LED) para indicar estado (ligado/desligado), quando aplicável.

2.6. ACIONADOR TIPO CHAVE PULSO

2.6.1. Deverá possuir acionamento manual por chave com retorno automático (momentâneo);

2.6.2. Permite liberação temporária da porta enquanto a chave estiver girada;

2.6.3. Indicado para situações que exigem controle rápido e seguro, sem manter circuito energizado;

2.6.4. Deve possuir cilindro metálico de alta durabilidade;

2.6.5. Placa frontal metálica com acabamento resistente à corrosão;

2.6.6. Compatível com sistemas de controle de acesso e travas eletromecânicas;

2.6.7. Instalação embutida ou sobreposta em batentes ou caixas padrão elétrica;

2.6.8. Sinalização visual (LED) para indicar acionamento, quando aplicável.

ANEXO I-D

ESPECIFICAÇÕES TÉCNICAS DO SISTEMA DE GERADOR DE NEBLINA

1. CARACTERÍSTICAS ESPECÍFICAS DO SISTEMA DE GERADOR DE NEBLINA

1.1 Deve permitir a programação de tempos de disparo e faixa horária de acionamento;

1.2 Deve possuir funções de configuração remota dos recursos nativos do equipamento;

1.3 Deve oferecer possibilidade disparos automáticos pela combinação de eventos, local (offline) ou remotamente, além de disparos e inibições por comando manual remoto.

2. EQUIPAMENTO

2.1 Deve ser construído em bloco de metal, permitindo instalação vertical ou horizontal, fixado em paredes, tetos ou embutido no forro, conforme infraestrutura local;

2.2 Deverá possuir componentes eletrônicos dedicados e integrados para armazenamento do firmware e funcionalidades da placa e que mitigue a eventualidade de corrupção;

2.3 Os recursos de controle, supervisão e acionamento do equipamento deverão ser implementados em hardware embarcado dedicado do fabricante;

2.4 A instalação deve ocorrer sem necessidade de opcionais não inclusos no projeto original do fabricante;

2.5 Quando fixado diretamente na parede ou teto, os elementos de fixação não devem ser acessíveis externamente. Em caso de violação, deve gerar sinal de alarme identificável pelo sistema de monitoramento;

2.6 Deve permitir alimentação elétrica conforme rede local;

2.7 Deve ser fornecido com fonte e bateria, garantindo funcionamento mínimo de 2 horas após queda de energia AC;

2.8 Deve possuir modo de economia de energia para reduzir custos quando em modo de espera (desarmado);

2.9 Deve ter sistema de autodiagnóstico com alarmes técnicos, informando problemas localmente e remotamente;

2.10 Deve possuir proteção contra violação do gabinete e suportes, incluindo grelhas quando instalado acima do forro;

2.11 Para evitar risco de incêndio, deve ter disjuntor térmico para desligar automaticamente elementos geradores de calor, independentemente dos circuitos eletroeletrônicos;

2.12 Deve possuir LEDs indicativos de funcionamento;

2.13 Deve permitir disparos sequenciais para inibir a visão;

2.14 Deve possuir sensor de obstrução do bico de saída de fluído, informando tentativa de bloqueio;

2.15 O acesso para reposição do fluído deve ser simples, sem necessidade de desinstalação do equipamento;

2.16 Deve possuir protocolo de comunicação para programação, disparo e análise via Ethernet ou pelos sistemas de alarme fornecido;

2.17 Deve possuir bornes para interligação via contato seco, informando disparo, níveis de fluído, falhas e violação;

2.18 O fluído deve restringir visibilidade a no máximo 20 cm em todas as direções, em até 30 segundos, preenchendo ambiente de 100 m³ (variação aceitável de ±10%);

2.19 A neblina deve persistir por no mínimo 20 minutos em ambiente sem ventilação forçada, mantendo as condições acima;

2.20 Após dissipação, não deve deixar resíduos, umidade ou elementos sólidos/líquidos nas superfícies;

2.21 O fluído deve ser compatível com o gerador, atóxico, com informações do fabricante;

2.22 Devem ser apresentados laudos de certificação emitidos por entidades independentes, comprovando que a toxicidade não excede limites nocivos à saúde ou meio ambiente;

2.23 O fornecedor deve apresentar dados de segurança do fluído emitidos pelo fabricante;

2.24 Deve permitir disparos programáveis em segundos;

2.25 Deve efetuar no mínimo 6 disparos com quantidade suficiente para proteger o volume especificado;

2.26 Deve ser fornecido com carga de líquido e permitir reabastecimento ou troca conforme recomendações do fabricante.

ANEXO I-E

ESPECIFICAÇÕES DOS SWITCHES

1 OBJETIVO

Equipamento de acesso para interligação de painéis de alarme, controladoras de acesso e dispositivos IP, com gerenciamento e segurança corporativa, visando aderência ao padrão de switches implantados na rede corporativa do Banco do Nordeste.

2 NECESSIDADE DE AQUISIÇÃO NA CAMADA DE ACESSO À REDE LOCAL (SWITCHES)

2.1 Possuir LED's indicativos do estado de funcionamento do equipamento;

2.2 Possibilitar a obtenção de estatísticas de tráfego e falhas das portas para todas as portas;

2.3 Estar equipados com recursos que permitam a reconfiguração dinâmica das diversas portas e módulos, inclusive permitindo a ativação e desativação de portas e módulos sem causar reinício, instabilidade ou qualquer impacto que venha a comprometer o funcionamento do equipamento;

2.4 Implementar ajuste de clock utilizando NTP (Network Time Protocol);

2.5 Permitir a atualização de versões de código utilizando os protocolos File Transfer Protocol (FTP) ou Trivial File Transfer Protocol (TFTP);

2.6 Permitir enviar logs para servidores remotos (Syslog);

2.7 Implementar traceroute para o descobrimento do caminho seguido por um pacote dentro da rede;

2.8 Todas as portas deverão ser autoconfiguráveis MDI/MDIX dispensando o uso de cabos cross over ou qualquer configuração para conexão a outro switch;

2.9 Permitir que um conjunto de switches seja administrado por único endereço IP;

2.10 O número de switches trabalhando em conjunto deverá ser de no mínimo 8 (oito);

2.11 Suportar protocolo para cópias seguras de arquivos de configuração do switch, seja Secure Copy Protocol (SCP) ou Secure File Transfer Protocol (SFTP);

2.12 Estar equipados com recursos que implementem funcionalidades de gerenciamento relativas ao padrão de gerenciamento SNMP (Simple Network Management Protocol), com suporte a RFC 1213 (MIB-II). Suporte ao SNMP v3;

2.13 Suportar configuração NETCONF ou Provisionamento Zero-Touch (ZTP) através do software de gerência;

2.14 Permitir a monitoração de desempenho de tráfego entre o switch e outro equipamento via MIB SNMP;

2.15 Implementar mecanismos de monitoramento e análise local e remota de tráfego em portas de switches pertencentes a uma mesma VLAN, através de configuração de espelhamento de portas;

2.16 Suportar o Link Layer Discovery Protocol (LLDP) e LLDP for Media Endpoint Devices (LLDP-MED): Padrão do IEEE para descobrimento de dispositivos em nível de enlace em redes Ethernet;

2.17 Estar equipados com 1 (uma) porta de comunicação out-of-band para gerenciamento de configuração, podendo essa ser uma porta serial, ou isolar uma porta de comunicação do switch através de uma VLAN, tornando a porta totalmente isolada do ambiente de acesso;

2.18 Permitir o gerenciamento através de Command Line Interface (CLI);

2.19 Permitir o gerenciamento através de web browser com suporte a SSL (Secure Socket Layer) versão 3 ou/e SSH (Secure Shell) versão 2;

2.20 Permitir o gerenciamento através de TELNET;

2.21 Permitir implementação de autenticação centralizada de controle de acesso dos equipamentos através de RADIUS ou TACACS+ (ou padrão compatível);

2.22 Possuir estrutura apropriada para acondicionamento em armário de fiação (rack) de 19 polegadas, ocupando uma unidade (1U), sendo incluso o fornecimento dessas peças para prender no rack, conhecidas como “orelhas” por exemplo, ou trilhos, mantendo 1U;

2.23 Possuir a capacidade de encaminhamento de, no mínimo, 80 milhões de pacotes por segundo (pacotes de 64 bytes), na camada 2 (dois) ou camada 3 (três), quando aplicável (modelo de referência OSI);

2.24 A matriz de comutação (Switch Fabric) deverá ter capacidade de throughput mínima de 100 (cem) gigabits por segundo;

2.25 A quantidade de memória DRAM (ou SDRAM) que o equipamento deve possuir (em gigabytes) deve ser de no mínimo 1 (um);

2.26 A quantidade de memória Flash que o equipamento deve possuir (em megabytes) é de no mínimo 512 (quinhentos e doze);

3 MÓDULOS / PLACAS DE INTERFACES REQUERIDOS

3.1 LAN: 10/100/1000 Mbps, interfaces RJ-45, para cabos UTP categoria 6 ou superior, full duplex, GigaEthernet, autosense, de acordo com os protocolos padrões Ethernet IEEE 802.3 10BaseT, Ethernet IEEE802.3u 100BaseTX, Ethernet IEEE802.3ab 1000BaseT.

4 QUANTIDADE DE PORTAS INSTALADAS

4.1 quantidade mínima de portas com interfaces RJ-45, para cabos UTP categoria 6, 10/100/1000BaseTX, full duplex, ethernet, autosense, que deverão estar instaladas em cada comutador (switch), para conexão de equipamentos: 12 (doze);

4.2 quantidade mínima de slots SFP, para cabos LC, Gigabit, que deverão estar instaladas em cada comutador (switch), para conexão de uplink: 2 (dois). Deverão ser entregues 2 transceivers Gigabit SFP para fibras LC multimodo.

5 REQUISITOS DE SEGURANÇA

5.1 Os equipamentos devem implementar o gerenciamento de configuração através da porta de gerenciamento com processo de autenticação e identificação positiva ou implementar o

gerenciamento de configuração através da porta de gerenciamento out-of-band ou xmodem (console) com processo de autenticação e identificação positiva;

5.2 Deverá permitir a aplicação de templates/baselines do Banco do Nordeste, para gerenciamento integrado da TI corporativa, incluindo soluções de NAC;

5.3 Deverá permitir a criação de listas de acesso baseadas em endereços IP para limitar o acesso ao switch via Telnet. Deve ser possível definir os endereços IP de origem das sessões Telnet e SSH;

5.4 Deverá implementar ACLs baseadas em Portas (Ethernet) Físicas do switch;

5.5 Deverá implementar ACLs baseadas em tempo;

5.6 Deverá implementar autenticação de login/senha para a liberação de tráfego na porta através do protocolo IEEE 802.1x com as seguintes funcionalidades:

5.6.1 atribuição de VLAN conforme a autenticação do usuário;
5.6.2 reautenticação forçada de todas as portas;
5.6.3 reautenticação periódica e definição de período de inatividade após falha de autenticação.

5.7 Deverá permitir a configuração de portas confiáveis e não confiáveis de forma a manter uma tabela correlacionando informações como porta, VLAN, IP, MAC para cada interface não confiável. Os servidores DHCP, por exemplo, devem estar conectados a interfaces confiáveis, pois qualquer resposta a uma solicitação DHCP será descartada em interfaces não confiáveis. Tal funcionalidade garante maior segurança e controle das redes LAN;

5.8 Deverá implementar mecanismos de Authentication, Authorization e Accounting (AAA) com garantia de entrega dos pacotes transferidos entre cliente e servidor AAA;
5.9 Todos os pacotes enviados ao servidor de controle de acesso e não só os pacotes referentes à senha;

5.10 Deverá permitir controlar quais comandos os usuários e grupos de usuário podem executar nos equipamentos gerenciados. Devem ser registrados no servidor AAA todos os comandos executados, assim como todas as tentativas de execução de comandos não autorizadas feitas por usuários que tiverem acesso ao equipamento gerenciado;

5.11 Deverá utilizar o protocolo TCP para prover maior confiabilidade ao tráfego dos envolvidos no controle administrativo;

5.12 Deverá permitir autenticação mútua entre o servidor AAA e o cliente AAA;

5.13 Deverá implementar mecanismos ao nível de porta de acesso que bloqueiem pacotes BPDUs inesperados;

5.14 Deverá possuir capacidade de limitação de endereços MAC por porta, acessíveis em uma dada interface de LAN do switch;

5.15 Deverá suportar a visualização de endereços MAC aprendidos pelo switch;

5.16 Caso um MAC seja remanejado (fisicamente) para outra porta do switch, ou para outro switch na rede, o switch deverá de forma dinâmica entender a movimentação desse MAC não sendo necessário nenhum comando manual ou qualquer outro procedimento que não seja automático para que o switch aprenda o novo local do MAC;

5.17 Deverá implementar a associação de um endereço MAC específico a uma dada porta do Switch, de modo que somente a estação que tenha tal endereço possa usar a referida porta para conexão;

5.18 Deverá possibilitar controle de broadcast por porta através de comando específico. Não será permitido o controle de broadcast por porta através de ACL (Access Control List). O controle deve ser compatível com IPv4 e IPv6;

5.19 Deverá possibilitar controle de multicast por porta através de comando específico. Não será permitido o controle de multicast por porta através de ACL (Access Control List). O controle deve ser compatível com IPv4 e IPv6;

5.20 Deverá implementar API de gerenciamento remoto, acessível via rede IP, documentada pelo fabricante, permitindo leitura e escrita de configurações, criação, alteração e remoção de VLANs, interfaces, ACLs e parâmetros de segurança, com autenticação segura. A API deve ser baseada em padrões abertos como REST/RESTCONF/NETCONF ou equivalente amplamente documentado, compatível com ferramentas de automação de mercado (ex.: Ansible, scripts Python);

5.21 As capacidades mínimas de VLAN, MAC address, ACLs, SNMP, espelhamento e QoS deverão ser suportadas de forma simultânea, sem degradação de desempenho.

6 PROTOCOLOS E PADRÕES REQUERIDOS

6.1 Deverá implementar, além dos padrões necessários para os requisitos desse edital, os seguintes protocolos e padrões:

6.1.1 IEEE 802.3, 10BaseT;
6.1.2 IEEE 802.3u, 100BaseTX;
6.1.3 IEEE 802.3ab, 1000BaseT;
6.1.4 IEEE802.3x, Flow Control;
6.1.5 IEEE 802.1q, VLAN Tagging;
6.1.6 IEEE 802.1d, SpanningTree;
6.1.7 IEEE 802.1s, Multiple Spanning Tree;
6.1.8 IEEE 802.3ad, Link Aggregation;
6.1.9 IEEE 802.1x, Port-Level Security;
6.1.10 IEEE 802.1w, Rapid Spanning Tree.

6.2 Deverá implementar mecanismos de minimização do tempo de convergência de Spanning-Tree em caso de falha de enlace ou switch da rede local, e as seguintes funcionalidades: configuração da porta para o estado de forwarding automaticamente, manutenção da raiz do Spanning-Tree (Root Guard ou Root Protection) e detecção de tráfego Spanning-Tree com opção de desabilitação da porta em caso de detecção positiva;

6.3 Deverá implementar proteção de BDPU por portas que de acordo com configuração irá permitir ou não o recebimento de BPDU na interface. Deverá ser possível configurar desativação automática da porta para proteção caso receba BDPU (recurso BPDU Guard ou equivalente), e deverá ser possível somente filtrar ou desconsiderar a BDPU (recurso BPDU filter ou equivalente). Para as portas desativadas por recebimento de BPDU, se configurada dessa forma, deverá ser possível o retorno automático das portas, ou seja, a reativação das interfaces, sem a necessidade de atuação manual;

6.4 Deverá implementar quadros ethernet de no mínimo 4000 bytes (Jumbo Frames) nas portas Gigabit Ethernet.

7 VLANS (Virtual LANs)

7.1 A quantidade mínima de VLAN's que deverão ser suportadas deve ser de 4000 (quatro mil);

7.2 Deveráimplementar o protocolo de trunking IEEE 802.1q para que o tráfego de várias VLANs possa passar por um enlace. O switch deve implementar protocolo de negociação de trunking.

8 QUALIDADE DE SERVIÇO

8.1 Deverá possuir 4 (quatro) filas em cada porta. Estas portas devem implementar os seguintes algoritmos de processamento de filas:

8.1.1 Weighted Round Robin (WRR) ou Shaped Round Robin (SRR) ou similar;

8.1.2 Deverá permitir a classificação de tráfego baseada em IEEE 802.1p.

9 MAC ADDRESS

9.1 A quantidade de MAC address que poderão ser utilizados simultaneamente deverá ser de no mínimo 8000 (oito mil).

10 AGREGAÇÃO DE PORTAS

10.1 Deverá implementar o aumento da largura de banda (nas ligações para comutador (switch) de núcleo e de acesso e para microcomputadores), através da agregação de múltiplas portas físicas funcionando como uma única porta lógica, conforme padrão IEEE 802.3ad. Este requisito valerá para todas as portas descritas no item “MÓDULOS / PLACAS DE INTERFACES SUPORTADOS”;

10.2 O switch deve implementar o protocolo de negociação Link Aggregation Control Protocol (LACP);

11 MULTICAST

11.1 Deverá implementar funcionalidades de IP multicast via Internet Group Management Protocol (IGMP) snooping versões 1, 2 e 3 do IGMP;

11.2 Deverá suportar no mínimo 128 grupos IGMP.

12 DHCP

12.1 Deverá implementar funcionalidades de Dynamic Host Configuration Protocol (DHCP) snooping e DHCP Server.

13 SISTEMA DE ALIMENTAÇÃO

13.1 Deverá possuir fonte de alimentação interna que trabalhe em 110V e 220V, 50/60 Hz, com detecção automática de tensão e frequência;

13.2 Deverá possuir ventilação ativa através de um ou mais ventiladores para dissipação de calor. Deve possuir também ajuste inteligente de velocidade.

ANEXO I-F

CADERNO DE TESTES

1. OBJETIVO

1.1. Estabelecer os procedimentos para avaliação técnica da amostra apresentada pela LICITANTE classificada provisoriamente em primeiro lugar, com o objetivo de verificar e comprovar a aderência funcional da solução ofertada em relação aos requisitos e especificações definidos no Edital e seus Anexos.

1.2. A avaliação será conduzida por meio de demonstrações práticas em ambiente de bancada, utilizando os equipamentos dos subsistemas que compõem a solução ofertada, devidamente integrados e operacionais, permitindo a validação de suas funcionalidades.

2. CRITÉRIOS GERAIS

2.1. No momento da apresentação da amostra e demonstração das funcionalidades, o LICITANTE deverá disponibilizar todos os materiais, equipamentos, acessórios, cabos, fontes de alimentação, softwares, licenças e demais recursos necessários ao pleno funcionamento da solução ofertada, em rede de dados estruturada própria, incluindo servidores, serviços e demais ativos para seu adequado funcionamento, não podendo alegar, em qualquer hipótese, a necessidade de fornecimento de qualquer item pelo BANCO, para viabilizar a realização dos testes e da avaliação técnica;

2.2. Deverão ser apresentados os equipamentos e itens correspondentes a todos os anexos do Edital, de forma integrada e estruturada para testes em bancada, permitindo a análise das principais funcionalidades e, quando aplicável, a simulação dos fluxos operacionais do sistema, conforme critérios de avaliação definidos pelo BANCO, conforme descrito a seguir:

- sistema integrado e operacional;
- central de alarme;
- controladora de acesso;
- leitora biométrica facial;
- gerador de neblina;
- switch;
- softwares;
- licenças;
- acessórios;
- cabeamentos;
- demais itens necessários à demonstração.

2.3. Os testes serão realizados nas dependências do BANCO;

2.4. O BANCO poderá, a seu exclusivo critério, solicitar a repetição de qualquer teste quando julgar necessário para a adequada comprovação das funcionalidades, do desempenho ou da conformidade da solução ofertada;

2.5. Para cada teste relacionado a seguir no item 5, serão verificadas também as características técnicas do(s) equipamento(s) envolvido(s), conforme previstas e relacionadas nos respectivos anexos de especificações técnicas, podendo ser por meio de comprovações em catálogo do equipamento/manual/datasheet ou aferição em bancada

3. CRITÉRIO DE AVALIAÇÃO

3.1. Para cada teste serão adotados os seguintes resultados:

Resultado	Significado
Aprovado	Funcionalidade demonstrada conforme solicitado
Reprovado	Funcionalidade não demonstrada ou demonstrada parcialmente

3.2. A reprovação da amostra em qualquer um dos testes ou critérios de avaliação previstos implicará sua imediata desclassificação, ficando o BANCO dispensado da realização dos demais testes, sem prejuízo do registro dos resultados já obtidos.

4. REGISTRO DE EVIDÊNCIAS

4.1. Durante a execução dos testes, a Comissão de Avaliação poderá registrar fotografias, capturas de tela, registros de auditoria, relatórios, vídeos, gravações das demonstrações ou quaisquer outras evidências consideradas necessárias para subsidiar sua análise técnica;

4.2. As evidências produzidas durante a avaliação poderão compor o processo administrativo da contratação e servir como elemento de fundamentação para aprovação ou reprovação da amostra apresentada pela LICITANTE;

4.3. Toda a sessão de apresentação e avaliação da amostra será registrada por meio do circuito fechado de televisão (CFTV) do BANCO, com gravação de áudio e vídeo, para fins de documentação e rastreabilidade do processo de avaliação técnica.

5. TESTES

SISTEMA INTEGRADO

5.1. TESTE 01 – Demonstração do Sistema

- Objetivo: Validar a capacidade da plataforma integrada de apresentar, de forma centralizada e em tempo real, os dispositivos, eventos, alarmes e estados operacionais dos subsistemas monitorados, permitindo ao operador identificar, acompanhar e tratar, de maneira eficiente, ocorrências operacionais, eventos críticos e situações de exceção.

- Metodologia: A LICITANTE deverá demonstrar o funcionamento da plataforma de monitoramento e supervisão da solução ofertada, evidenciando sua capacidade de integração, visualização e gerenciamento operacional. A demonstração deverá contemplar, no mínimo, as seguintes funcionalidades:

  - visualização simultânea dos subsistemas integrados;
  - apresentação dos eventos em tempo real;
  - identificação dos dispositivos monitorados;
  - visualização dos estados operacionais dos equipamentos;
  - identificação e tratamento de alarmes ativos;
  - utilização de mapas gráficos, dashboards ou recursos equivalentes de monitoramento disponibilizados pela solução;
  - navegação entre os eventos e elementos monitorados.

- Resultado Esperado: A solução deverá demonstrar capacidade de monitoramento centralizado dos sistemas integrados, apresentando, de forma organizada, intuitiva e em tempo real, os dispositivos, eventos, alarmes, e respectivos estados operacionais dos subsistemas integrados, permitindo ao operador identificar, localizar, acompanhar e tratar os eventos por meio de interface única de operação.

5.2. TESTE 02 – Gestão de Usuários

- Objetivo: Validar os mecanismos de cadastro, sincronização e administração de usuários, operadores grupos e perfis de acesso, bem como a correta aplicação das permissões e restrições definidas para cada perfil.

- Metodologia: Realizar:

  - inclusão de usuário;
  - sincronização por AD/LDAP ou mecanismo equivalente;
  - atribuição de perfis distintos de acesso;
  - visualização das permissões associadas aos perfis.

- Resultado Esperado: A solução deverá demonstrar a capacidade de gerenciamento de usuários, operadores, credenciais e perfis hierarquizados, assegurando a correta aplicação das permissões e restrições associadas a cada perfil. Deverá, ainda, evidenciar o funcionamento dosmecanismos de integração e sincronização previstos nas especificações técnicas, garantindo a consistência dos dados e a adequada administração dos acessos à plataforma.

5.3. TESTE 03 – Mapas Gráficos Interativos e Localização de Eventos

- Objetivo: Validar a capacidade da plataforma integrada de representar graficamente os dispositivos monitorados, permitindo a identificação visual dos equipamentos, seus estados operacionais e a localização de eventos em ambiente gráfico interativo.

- Metodologia: A LICITANTE deverá demonstrar o funcionamento do recurso de mapa gráfico, planta baixa, representação geográfica ou funcionalidade equivalente disponibilizada pela solução:

  - cadastro ou apresentação de ambiente gráfico contendo dispositivos monitorados;
  - representação gráfica de ao menos um ponto de acesso controlado;
  - representação gráfica de ao menos um dispositivo de alarme;
  - indicação visual do estado operacional dos dispositivos;
  - localização gráfica de eventos gerados durante a demonstração;
  - atualização automática das informações apresentadas no mapa em função da ocorrência dos eventos;
  - navegação entre os elementos representados no ambiente gráfico.

- Resultado Esperado: A solução deverá demonstrar recurso de monitoramento gráfico interativo, permitindo a identificação visual dos dispositivos monitorados e dos eventos a eles associados. Os eventos gerados pelos subsistemas integrados deverão ser apresentados de forma correlacionada aos elementos gráficos correspondentes, possibilitando ao operador identificar rapidamente sua origem, localização e estado operacional por meio da mesma interface de monitoramento. O ambiente gráfico deverá refletir, de forma dinâmica e em tempo real, as alterações de estado dos dispositivos e os eventos produzidos pelos subsistemas integrados, assegurando a atualização automática das informações apresentadas e o suporte às atividades de monitoramento, supervisão e tratamento de ocorrências.

5.4. TESTE 04 – Relatórios Operacionais e Auditoria

- Objetivo: Validar a capacidade da plataforma integrada de consultar, consolidar, filtrar, gerar e exportar informações operacionais e de auditoria, possibilitando o acompanhamento dos eventos gerados pelos subsistemas monitorados.

- Metodologia: A LICITANTE deverá demonstrar a geração de relatórios operacionais e de auditoria contendo informações provenientes dos subsistemas apresentados durante a demonstração. Deverão ser evidenciados, no mínimo, os seguintes recursos:

  - aplicação de filtros por período;
  - aplicação de filtros por unidade ou local monitorado;
  - aplicação de filtros por usuário, operador, visitante ou credencial;
  - aplicação de filtros por dispositivo ou ponto de acesso;
  - aplicação de filtros por tipo de evento;
  - consulta de eventos específicos ocorridos durante a demonstração da solução.

  Os relatórios gerados deverão apresentar, quando aplicável, as seguintes informações:

  - identificação do relatório;
  - data e hora da emissão;
  - período de referência;
  - unidade ou local monitorado;
  - identificação do usuário, operador, visitante ou credencial relacionada ao evento;
  - tipo de evento registrado;
  - data e hora de ocorrência;
  - status do evento;
  - identificação do operador ou sistema responsável pela ação registrada.

  Adicionalmente, a LICITANTE deverá ainda demonstrar a exportação de pelo menos um relatório nos formatos: PDF, CSV e XLSX.
  Resultado Esperado: A solução deverá permitir a geração de relatórios operacionais e de auditoria com filtros parametrizáveis, contemplando as informações registradas pelos subsistemas integrados.

SISTEMA DE ALARME

5.5. TESTE 05 – Detecção e Monitoramento de Eventos

- Objetivo: Validar a capacidade do sistema de alarme de detectar eventos gerados pelos dispositivos de campo e transmitir as respectivas informações para a plataforma integrada de monitoramento.

- Metodologia: A LICITANTE deverá gerar eventos de alarme por meio do acionamento de sensores e dispositivos conectados à central de alarme apresentada na demonstração, evidenciando o processamento e a transmissão das ocorrências pela solução.

- Resultado Esperado: Os eventos gerados deverão ser recebidos, processados e apresentados na plataforma integrada de monitoramento em tempo real, contendo as informações necessárias para identificação da origem, tipo e estado da ocorrência.

5.6. TESTE 06 – Arme e Desarme Remoto

- Objetivo: Validar a execução de comandos remotos.

- Metodologia: Realizar operações de arme e desarme por meio da plataforma integrada.

- Resultado Esperado: A central deverá alterar corretamente seu estado operacional, com o respectivo registro da ação nos mecanismos de auditoria da solução.

5.7. TESTE 07 – Supervisão dos Dispositivos

- Objetivo: Validar o monitoramento da disponibilidade operacional dos dispositivos.

- Metodologia: Simular a indisponibilidade de um dispositivo supervisionado.

- Resultado Esperado: A solução deverá identificar a indisponibilidade do dispositivo e gerar o correspondente evento de falha na plataforma integrada.

5.8. TESTE 08 – Operação Offline

- Objetivo: Validar funcionamento local na ausência de comunicação com o servidor.
- Metodologia: Simular indisponibilidade da comunicação IP.
- Resultado Esperado: A solução deverá manter o funcionamento local dos dispositivos e registrar os eventos gerados durante a indisponibilidade, realizando sua sincronização automática com a plataforma após o restabelecimento da comunicação.

SISTEMA DE CONTROLE DE ACESSO

5.9. TESTE 09 – Autenticação Biométrica Facial

- Objetivo: Validar reconhecimento biométrico facial, para autenticação de usuários.
- Metodologia: Realizar autenticação utilizando usuário previamente cadastrado na solução.
- Resultado Esperado: Reconhecimento e autorização do acesso.

5.10. TESTE 10 – Detecção de Vivacidade

- Objetivo: Validar os mecanismos de proteção contra fraude biométrica.
- Metodologia: Apresentar fotografia, imagem estática ou outro recurso de simulação perante a leitora, conforme funcionalidades previstas pelo fabricante do equipamento.
- Resultado Esperado: A tentativa de autenticação deverá ser rejeitada, impedindo a liberação do acesso.

5.11. TESTE 11 – Operação Offline

- Objetivo: Validar o funcionamento do sistema de controle de acesso na ausência de comunicação com o servidor.
- Metodologia: Simular a interrupção da comunicação entre o controlador e o servidor da solução.
- Resultado Esperado: Validação das regras locais e continuidade do controle de acesso.

5.12. TESTE 12 – Regra de Acesso de Circulação

- Objetivo: Validar mecanismos de controle de circulação, configuradas na solução.
- Metodologia: Realizar tentativas consecutivas de entrada sem o respectivo registro de saída correspondente.
- Resultado Esperado: A solução deverá aplicar a regra configurada e bloquear a nova tentativa de acesso quando aplicável.

5.13. TESTE 13 – Regra de Dupla Custódia

- Objetivo: Validar acesso condicionado à autenticação de múltiplos usuários.

- Metodologia: Configurar acesso com exigência de autenticação de dois usuários.
- Resultado Esperado: Liberação somente após autenticação dos usuários exigidos pela regra configurada.

5.14. TESTE 14 – Abertura Remota Assistida

- Objetivo: Validar fluxo de atendimento pela Central de Segurança.
- Metodologia: Gerar solicitação de acesso remoto, por meio da solução.
- Resultado Esperado: A Central de Segurança deverá visualizar a solicitação, consultar as informações associadas ao usuário e realizar a liberação remota do acesso, com o respectivo registro da operação.

SISTEMA DE GERADOR DE NEBLINA

5.15. TESTE 15 – Supervisão Operacional

- Objetivo: Validar monitoramento do equipamento.
- Metodologia: Consultar os estados operacionais, alarmes e eventos disponibilizados pelo equipamento na plataforma.
- Resultado Esperado: A solução deverá apresentar, de forma correta e em tempo real, os estados operacionais, alarmes e eventos do gerador de neblina na plataforma integrada.

5.16. TESTE 16 – Acionamento Remoto e Automático

- Objetivo: Validar capacidade de disparo remoto.
- Metodologia: Executar comando remoto de acionamento do gerador de neblina.
- Resultado Esperado: O equipamento deverá reconhecer e executar corretamente o comando recebido, registrando o evento correspondente na plataforma integrada.

TESTES DE INTEGRAÇÃO

5.17. TESTE 17 – Integração com Sistemas de CFTV e Fechadura de Retardo

- Objetivo: Validar a capacidade da plataforma integrada ofertada de interoperar com os sistemas corporativos previstos nas especificações técnicas do Banco do Nordeste, especificamente o sistema de videomonitoramento ISS SecurOS® e o sistema de fechadura de retardo randômico SGS InterGard®, permitindo o monitoramento, correlação, tratamento e rastreabilidade dos eventos provenientes desses sistemas.
- Metodologia: Deverá disponibilizar, durante a apresentação da amostra, todos os equipamentos, softwares, licenças, integrações, simuladores, máquinas virtuais e demais recursos necessários à demonstração da funcionalidade, não sendo admitida dependência de infraestrutura do BANCO:

  Integração com o sistema ISS SecurOS®

  - associação de eventos gerados pelo Sistema Integrado a câmeras previamente cadastradas;
  - apresentação automática da imagem, vídeo ao vivo ou gravação associada ao evento;
  - correlação entre eventos operacionais e respectivos recursos de vídeo;

- visualização, em interface operacional unificada, do evento e da câmera correspondente.

Integração com o sistema SGS InterGard®

- demonstração do recebimento e tratamento de eventos provenientes do sistema de fechadura de retardo randômico;
- apresentação dos estados operacionais disponibilizados pela integração;
- demonstração da recepção, visualização e tratamento de eventos de abertura, fechamento, bloqueio, violação, porta aberta por tempo superior ao configurado e demais eventos suportados pela integração.

- Resultado Esperado: A plataforma deverá demonstrar integração funcional com os sistemas ISS SecurOS® e SGS InterGard®, possibilitando o recebimento, monitoramento, visualização, correlação e tratamento centralizado dos eventos provenientes desses sistemas. Os eventos deverão ser apresentados em interface única, com rastreabilidade operacional e registros de auditoria compatíveis com as funcionalidades previstas nas especificações técnicas. A comprovação poderá ocorrer por meio de integração efetiva ou ambiente de demonstração provido pela LICITANTE, desde que represente fielmente os fluxos operacionais previstos para a solução.

5.18. TESTE 18 – Correlação de Eventos

- Objetivo: Validar a capacidade da plataforma de correlacionar eventos e executar ações automáticas entre os entre subsistemas da solução.

- Metodologia: A LICITANTE deverá demonstrar e criação e execução de regras entre os subsistemas apresentados, por meio dos eventos gerados pelos sistemas de alarme, controle de acesso ou gerador de neblina, desencadear ação ao outro, a exemplo:

  - Evento de sensor de fumaça acionando a liberação de porta controlada;
  - Violação de porta controlada acionando a sirene do sistema de alarme;
  - Disparo de gerador de neblina acionando a sirene de alarme.

- Resultado Esperado: A solução deverá demonstrar a correlação automática entre eventos e ações configuradas, apresentando os registros correspondentes na plataforma integrada e permitindo o acompanhamento centralizado das ocorrências e das respostas executadas.

5.19. TESTE 19 – Fluxo Operacional Completo

- Objetivo: Validar a operação integrada da solução durante um ciclo operacional completo de uma unidade, contemplando os principais procedimentos executados pela Central de Monitoramento e pelos usuários autorizados, desde a abertura até o encerramento das atividades da unidade.

- Metodologia: a LICITANTE deverá simular, em ambiente de demonstração, um cenário operacional completo de funcionamento de uma unidade, contemplando, no mínimo:

  - abertura da unidade;
  - desarme do sistema de alarme;
  - autenticação de usuários por meio do sistema de controle de acesso;
  - registro e tratamento dos eventos gerados durante a operação;
  - monitoramento dos eventos pela Central de Monitoramento;
  - execução de ações operacionais decorrentes dos eventos gerados;
  - encerramento das atividades da unidade;
  - rearme do sistema de alarme.

- Resultado Esperado: A solução deverá demonstrar funcionamento integrado e contínuo dos subsistemas envolvidos, permitindo o monitoramento, tratamento e acompanhamento dos eventos operacionais em interface centralizada, com registro auditável das ações executadas, dos usuários envolvidos e dos respectivos horários de ocorrência. Todo o fluxo operacional deverá ser rastreável por meio dos mecanismos de monitoramento e auditoria da plataforma.

5.20. TESTE 20 –Tratamento de Eventos e Fluxo de Trabalho

- Objetivo: Validar a capacidade da plataforma integrada de apoiar o processo de gerenciamento, acompanhamento, tratamento e encerramento de ocorrências operacionais, permitindo a rastreabilidade das ações executadas pelos operadores da Central de Monitoramento.

- Metodologia: A LICITANTE deverá demonstrar, no mínimo, as seguintes funcionalidades:

  - cadastrar ou configurar fluxo de trabalho, procedimento operacional ou mecanismo equivalente disponível na solução;
  - recebimento do evento pela plataforma integrada;
  - identificação do dispositivo ou subsistema responsável pela ocorrência;
  - visualização das informações associadas ao evento;
  - reconhecimento ou assunção do evento por operador autorizado;
  - registro de observações, comentários ou histórico operacional, quando disponível na solução;
  - alteração de status da ocorrência durante o ciclo de tratamento;
  - encerramento da ocorrência;
  - consulta posterior do histórico completo do atendimento realizado.

- Resultado Esperado: A solução deverá demonstrar recursos para gerenciamento e tratamento de ocorrências operacionais, permitindo o acompanhamento do evento desde sua geração até seu encerramento, preservando o histórico das ações executadas. Todas as ações realizadas durante o atendimento deverão permanecer registradas e disponíveis para consulta posterior, garantindo a rastreabilidade do processo, a identificação dos operadores envolvidos e o histórico completo da ocorrência.

ANEXO I-G

MEMORIAL DESCRITIVO DOS SERVIÇOS

1. OBJETIVO

Descrever os detalhes e características dos componentes, acessórios, materiais e outros tópicos pertinentes ao objeto da contratação, que se refere ao sistema integrado de segurança eletrônica, contemplando alarme, controle de acesso físico e gerador de neblina, incluindo o fornecimento por locação, com possibilidade de compra pelo BANCO, de todos os equipamentos eletrônicos, computacionais e seus acessórios, bem como aplicativos e suas licenças, além de provimento de infraestrutura civil e de dados complementares, quando necessária, serviços de instalação, treinamento, monitoramento da disponibilidade do sistema e seus componentes, manutenções *on site*, por fim, eventuais remanejamentos, reinstalações ou desinstalações de componentes/sistema nas unidades do BANCO. Este sistema deverá se integrar em sistemas corporativos de CFTV IP e fechadura com retardo para cofres já implantados no Banco do Nordeste, em conformidade com as especificações constantes do Edital e seus Anexos.

2. CARACTERÍSTICAS GERAIS

2.1. O Sistema Integrado de Segurança Bancária a ser contratada pelo BANCO é previsto para ser instalado em unidades de negócio e administrativas localizadas nos estados do AL, BA, CE, DF, ES, MA, MG, PB, PE, PI, RJ, RN, SE e SP;

2.2. Cada unidade receberá os equipamentos e quantitativos, de acordo com as especificações técnicas contidas no **Anexo** denominado **Rede de Unidades**, podendo haver, a critério do BANCO, a possibilidade de variações para mais ou menos, conforme as necessidades do BANCO;

2.3. Cada unidade possui uma sala de equipamentos, onde se encontram e convergem todos os recursos de Tecnologia da Informação (TI) da unidade. Na Sala de Equipamentos deverá ser instalada também toda a solução do CONTRATADO, incluindo central de alarme e módulos de controle de acesso em rack específico. Assim, a partir desse ponto ocorrerá todo o cabeamento de dados e elétrico, que se estenderão aos componentes do sistema;

2.4. Os equipamentos de TI que farão a gestão centralizada dos recursos do sistema, por sua vez, também deverão ser instalados na sala de equipamentos;

2.5. A conectividade das unidades à rede será provida pelo BANCO;

2.6. O switch deverá ser fornecido pelo CONTRATADO, atendendo as especificações contidas no **Anexo** denominado **Especificações dos Switches**;

2.7. O servidor central do Sistema Integrado de Segurança Bancária será fornecido pelo BNB no Data Center corporativo, em Fortaleza - CE. Trata-se de servidores virtuais, que terão dimensionamento computacional e configurações necessárias para a perfeita instalação e funcionamento da solução;

2.8. O BANCO possui uma Central de Segurança, que será a responsável pelo gerenciamento e monitoramento do Sistema Integrado de Segurança Bancária, que se encontra localizada também em Fortaleza - CE.

3. DOS EQUIPAMENTOS

3.1. Os componentes críticos da solução, responsáveis por controle, autenticação, monitoramento, armazenamento de configurações, processamento de eventos ou acionamento dos

subsistemas, deverão ser constituídos por equipamentos de propósito específico, desenvolvidos e suportados pelo fabricante da solução, não sendo admitidas implementações baseadas exclusivamente em plataformas de prototipagem ou desenvolvimento destinadas primordialmente a fins laboratoriais, educacionais ou experimentais;

3.2. Os equipamentos deverão possuir mecanismos próprios de proteção das configurações operacionais, identidades lógicas, parâmetros de funcionamento e firmware, de forma a reduzir riscos de adulteração, substituição não autorizada de componentes críticos ou restauração não controlada das configurações da solução;

3.3. Todos os equipamentos fornecidos deverão ser novos, de primeiro uso, sem histórico de instalação ou utilização anterior, devendo ser apresentada documentação que comprove sua origem e data de aquisição, quando solicitada pelo Contratante. Não serão aceitos equipamentos recondicionados, remanufaturados ou usados;

3.4. É de responsabilidade do CONTRATADO o fornecimento de todos os equipamentos, cabos de interconexões e acessórios para funcionamento pleno do Sistema Integrado de Segurança Bancária;

3.5. O módulo de controle de acesso deverá ser acondicionado, juntamente com a fonte de alimentação e bateria, em rack a ser fornecido pelo CONTRATADO;

3.6. O painel do sistema de alarme deverá ser acondicionado, juntamente com a fonte de alimentação e bateria, no mesmo rack dos demais equipamentos de rack fornecidos pelo CONTRATADO;

3.7. O local de instalação deverá ser na sala de equipamentos da unidade, ou área definida pelo BANCO, de acordo com o espaço disponível na área reservada de cada localidade;

3.8. Deverá ainda possuir fechadura com chave para se evitar acessos indevidos;

3.9. O gerador de neblina deverá ser instalado no forro da sala de Tesouraria e/ou no Salão de Autoatendimento, ou outros ambientes, a depender do projeto de segurança da unidade;

3.10. Os suportes e acessórios necessários para a devida fixação das fechaduras do sistema de controle de acesso físico deverão ser definidos de acordo com o tipo de porta;

3.11. As fontes de alimentação, no-breaks e baterias deverão ser dimensionadas pelo CONTRATADO de acordo com as especificações de consumo dos equipamentos;

3.12. As leitoras biométricas deverão ser instaladas nas proximidades das respectivas portas, pelo seu lado externo, de modo que seja possível a leitura facial e identificação, com altura no mínimo de 1,40m, em relação ao piso do ambiente;

3.13. As botoeiras de saída deverão ser instaladas no ambiente interno das respectivas portas, com altura de 1,40m em relação ao piso do ambiente;

3.14. O acionador de chave tipo pulso deverá ser instalado nas proximidades da Porta Auxiliar da PSDM (Porta de Segurança Detectora de Metais), pelo lado interno, com altura de 1,40 m em relação ao piso do ambiente;

3.15. O acionador de chave tipo alternada liga/desliga deverá ser instalada na área interna da unidade para liberação/travamento da Porta Principal, com altura de 1,40 m em relação ao piso do ambiente;

3.16. Os componentes do sistema de alarme deverão ser fixados em alturas e posições definidas pelo BANCO.

4. DA INFRAESTRUTURA

4.1. Deverão ser utilizadas a infraestrutura de calhas e eletrodutos já existentes do BANCO, devendo, se necessário, serem feitos os complementos e ajustes, sem comprometimento dos recursos existentes;

4.2. A infraestrutura que o BANCO proverá, refere-se a cabeamento UTP Cat 6, com conectores RJ 45, certificados para todos os pontos onde estarão distribuídos os componentes do sistema;

4.3. Caso não haja infraestrutura pronta ou adequada para algum ponto a ser instalado algum dos componentes do sistema, poderão ser utilizados outros recursos, em caráter provisório e enquanto a infraestrutura certificada pelo BANCO não for disponibilizada, devendo ser prevista a transposição para a infraestrutura definitiva, quando aplicável, às expensas do CONTRATADO;

4.4. Será provido também pontos de energia elétrica para os componentes que necessitarem, a exemplo de gerador de neblina e o próprio *no-break*;

4.5. São de responsabilidade do CONTRATADO o fornecimento de eventuais materiais complementares de infraestrutura civil, elétrica e lógica, necessários para a instalação e funcionamento pleno do sistema, devendo fazer parte da composição de preços da proposta comercial o fornecimento de acessórios e materiais necessários para as conexões dos equipamentos aos pontos de rede e energia fornecidos pelo BANCO, para as situações que couberem, além das interconexões entre os periféricos dos dispositivos a serem fornecidos;

4.6. Pode ser demandada a recomposição e acabamento em gesso, furação de lajes ou paredes, pinturas, entre outros, que se faça necessário para devida recomposição do status em que se encontrava as edificações das unidades;

4.7. Para melhor cumprimento do item anterior, se necessário, é de responsabilidade do CONTRATADO a remoção dos componentes do sistema de segurança legados de outras instalações, sinalizados pelo BANCO, incluindo eventuais cabos e infraestruturas obsoletas e inadequadas;

4.8. Se necessário, o lançamento dos cabos dos equipamentos deverá ser feito por sobre o forro dos blocos em eletrodutos de PVC, ou copex metálico revestido, com diâmetro de 1” (uma polegada), no mínimo, fixados no teto por abraçadeiras tipo D;

4.9. Para os dispositivos instalados sobrepostos em paredes ou divisórias, o encaminhamento deverá ser aparente, através de eletrocalhas e conexões de alumínio do tipo dutotec ou similar;

4.10. Toda fiação adicional deverá ser identificada através de anilhas plásticas;

4.11. É de responsabilidade do CONTRATADO a adequação necessária na estrutura das portas para fixação dos equipamentos e passagem de cabeamento, bem como o serviço de abertura e fechamento de forro, quando necessários;

4.12. Ao menos as portas de acesso principal e acesso a área de atendimento, constituem-se de material em vidro temperado, não suportando novas furações, devendo ser os equipamentos adaptáveis às furações existentes ou até mesmo sobreposto;

4.13. As distâncias envolvidas entre o local de instalação dos componentes periféricos e a sala de equipamentos ou do ponto de infraestrutura provida pelo BANCO, de cada ponto, poderão ser checadas durante a vistoria prévia, inclusive antes da contratação.

5. SERVIÇOS DE INSTALAÇÃO, LOCAÇÃO E DESINSTALAÇÃO

5.1. Todos os materiais e equipamentos deverão ser instalados observando-se as orientações legais, não será aceito materiais ou equipamentos que necessitem de adaptações que burlem as normas e padrões de instalações estabelecidos;

5.2. A ativação do Sistema Integrado de Segurança Bancária nas unidades relacionadas no Plano de Distribuição deverá seguir as etapas, conforme cronograma a definir, a partir da requisição formal do BANCO, por e-mail do Fiscal Administrativo ou Fiscal Técnico deste Contrato:

Etapa	Prazo Máximo em Dias Corridos
Reunião de abertura na sede do BANCO, em Fortaleza - CE, para repasse das orientações e procedimentos para entrega do objeto.	7
Envio do cronograma de instalação dos sistemas nas unidades e dados dos técnicos.	7
Instalação, configuração e ativação do sistema na Central de Monitoramento do BANCO, em Fortaleza - CE.	30
Instalação e Ativação do Sistema	150
Entrega por Demanda (outras Unidades fora do plano inicial de implantação)	20

5.3. Deverão ser dimensionadas pelo CONTRATADO tantas equipes quantas sejam necessárias para cumprimento do prazo acima;

5.4. Todas as instalações deverão ser executadas por funcionários do quadro do CONTRATADO, de forma que a subcontratação só seja permitida para auxiliares de serviços, ou seja, deverá, no mínimo, haver um responsável técnico do CONTRATADO presente em cada instalação, como forma de garantia de serviços esperados, padronização e responsabilidades direta do CONTRATADO;

5.5. Os prazos poderão ser postergados de acordo com a necessidade do BANCO;

5.6. Os prazos são iniciados por sinalização do Banco, por fiscal deste Contrato, por meio de e-mail, após o aceite da etapa anterior;

5.7. Os equipamentos deverão ser entregues ao BANCO prontos para uso, devendo ser utilizados de acordo com os manuais de operação, de forma cuidadosa e adequada, durante todo o período de vigência deste Contrato, cuidando para que se mantenham em bom estado de conservação;

5.8. A instalação dos equipamentos deverá obedecer ao cronograma fornecido pela empresa e autorizado pelo BANCO e ocorrerá de forma a não prejudicar as atividades normais nas Unidades, podendo os mesmos ser realizados de dia ou noite, o que melhor convier ao BANCO;

5.9. Para fins de dimensionamento das interconexões dos componentes dos sistemas, eles ficam distantes de 5 a 40 metros da Sala de Equipamentos, onde está situada a conectividade das unidades, onde também deverá ser instalada a central de alarme e módulos de controle de acesso e para onde convergem todos os equipamentos cabeados;

5.10. Ao final da instalação dos equipamentos nas Unidades, o CONTRATADO deverá realizar os procedimentos de testes, visando comprovação das funcionalidades do sistema e comunicação, devendo obrigatoriamente confirmar o resultado com a Central do BANCO;

5.11. Ao final dos testes, orientar os gestores sobre o uso do sistema e procedimentos para realização de testes (funcionalidades dos equipamentos etc.);

5.12. Decorrida ativação do sistema, enviar a ordem de serviço relativa ao processo, constatando conformidade com as especificações técnicas estabelecidas;

5.13. A instalação dos equipamentos deverá obedecer ao cronograma fornecido pela empresa e autorizado pelo BANCO e ocorrerá de forma a não prejudicar as atividades normais nas Unidades, devendo ser realizada fora do horário de expediente bancário, pós às 18h00, ou o que melhor convir ao BANCO;

5.14. Para que seja viabilizado o cumprimento do prazo contratual dos serviços, estes poderão ser desenvolvidos em horário de expediente de acordo com a conveniência do BANCO;

5.15. No caso de realização dos trabalhos em horário noturno, a Unidade deverá ser comunicada com antecedência de pelo menos 2 (dois) dias úteis;

5.16. Considerar que as unidades se encontram em funcionamento e que o desenvolvimento dos serviços do CONTRATADO não deverá acarretar transtornos à rotina de trabalho da instituição;

5.17. Os serviços prejudiciais ao funcionamento de determinado ambiente, p. ex. pelo barulho, poeira, desligamento de energia, retirada de forro etc., deverão ser acordados previamente com o BANCO;

5.18. Ao final da instalação dos equipamentos nas unidades, o CONTRATADO deverá recondicionar o local de intervenção para pleno funcionamento, incluindo limpeza e organização do ambiente; configurar o sistema, conforme padrão determinado pelo BANCO e cadastrar os usuários;

5.19. Realizar os procedimentos de testes visando comprovação das funcionalidades do sistema e das vias de comunicação, devendo, obrigatoriamente, confirmar o resultado com a Central de Monitoramento do BANCO e do CONTRATADO;

5.20. Emitir o termo de recebimento juntamente com o Gerente da unidade, enviando-o ao Ambiente de Segurança Corporativa, e-mail, conforme modelo constante a ser fornecido;

5.21. O termo de recebimento deverá ser assinado quando não houver mais pendências de instalação/configuração que dependam exclusivamente do CONTRATADO;

5.22. A partir do referido termo, os equipamentos estarão aptos para os serviços de locação;

5.23. Obriga-se o BANCO a proteger os equipamentos de qualquer perturbação ou esbulho e a não permitir que sejam penhorados ou onerados por qualquer motivo, dando ciência imediata ao CONTRATADO de qualquer ocorrência que possa constituir risco, prejuízo ou violação dos direitos sobre os equipamentos. Relativamente a estes fatos, obriga-se o BANCO a fornecer todas as informações e documentos de que dispuser;

5.24. Intervenções por alterações ou remanejamentos também serão de responsabilidade do CONTRATADO por ocasião de alterações de leiaute, mudança de endereço da agência ou quando houver autorização da área de Segurança do BANCO, caracterizando serviços eventuais, que serão aferidos em horas técnicas, conforme previsão contratual e detalhamento nos itens a seguir;

5.25. O(s) equipamento(s) somente poderá(ão) ser remanejado(s) internamente ou para outra Unidade do BANCO por técnico do CONTRATADO, inclusive em caso de reforma de agências;

5.26. No caso de chamados técnicos referentes a serviços eventuais, o CONTRATADO deverá providenciar em até 5 (cinco) dias;

5.27. São considerados serviços eventuais: remanejamentos, reconfigurações e ajustes in loco a pedido do Banco, visitas improdutivas, ou qualquer serviço sobre os equipamentos, que não ensejam em instalações, desinstalações e manutenções previstas nos pagamentos mensais;

5.28. Deverão ser faturados os valores dos serviços eventuais em notas avulsas ao faturamento mensal;

5.29. Deverão ser registradas as horas utilizadas para a execução dos serviços em ordem de serviço específica com detalhe por serviço e componente. O quantitativo de horas para aquele serviço sobre o componente será multiplicado pelo valor da hora técnica definida na planilha de custos eventuais;

5.30. Expirado o prazo de vigência do Contrato, caso não haja aquisição por parte do Banco, os equipamentos deverão ser retirados obrigatoriamente pelo CONTRATADO no prazo de 90 (noventa) dias;

5.31. O CONTRATADO deverá apresentar cronograma de desinstalação dos equipamentos, o qual deverá estar de acordo com o cronograma de instalação da nova empresa vencedora do certame, de forma a se evitar descontinuidade dos serviços.

6. VENDAS DE EQUIPAMENTOS, COMPONENTES E LICENÇAS de sistema

6.1. Ao término da vigência do contrato, o BANCO poderá exercer a opção de compra dos equipamentos, componentes e licenças de sistema objeto deste contrato;

6.2. Os equipamentos deverão estar plenamente funcionais;

6.3. A opção de compra deverá ser manifestada por escrito ao CONTRATADO com antecedência mínima de 60 dias antes do término da vigência contratual;

6.4. O valor residual do equipamento será resultante de 1% do valor global da locação pelos 60 meses;

6.5. O pagamento deverá ocorrer no 5º (quinto) dia útil, após formalização de aceite do BANCO, após a emissão da nota fiscal correspondente;

6.6. A propriedade dos equipamentos será transferida ao BANCO após pagamento integral do valor da opção de compra e entrega da documentação necessária pelo CONTRATADO;

6.7. Após a compra, cessam as obrigações de locação, aplicando-se as garantias previstas para aquisição definitiva.

7. MONITORAMENTO, MANUTENÇÃO E SUPORTE TÉCNICO

7.1. O CONTRATADO deverá possuir equipe devidamente treinada e estrutura física própria, dotada de telefone e correio eletrônico próprio, para a tomada de providências quanto eventos do sistema, bem como para assegurar que todos os outros recursos estejam em perfeitas condições de funcionamento, por meio de monitoração ativa, 24 horas por dia, durante 7 dias da semana, todas as unidades em contrato do BANCO;

7.2. Monitorar as funcionalidades do sistema e seus recursos, principalmente a ocorrência de eventos que possam comprometer seu regular funcionamento e conformidade, devendo eles serem tratados imediatamente, visando a plena disponibilidade;

7.3. Armazenar todas as ocorrências havidas e transmitidas pela central de alarme, no mínimo, nos últimos 12 (doze) meses;

7.4. O dimensionamento de volume de dados é de responsabilidade do CONTRATADO;

7.5. Possuir lista de procedimentos pré-definidos a serem tomados pelo operador de acordo com o tipo de ocorrência. Esses procedimentos deverão ser alinhados com o BANCO;

7.6. Permitir a perfeita identificação da Unidade de onde está sendo enviada a comunicação, vinculada a data e hora do evento (horário da ocorrência e horário de recebimento da informação), bem como do tipo da ocorrência, seja de supervisão ou de monitoração;

7.7. Possuir, disponibilizado pelo BANCO, cadastro com todas as unidades ativas do Banco, bem como dos usuários dos subsistemas em monitoração;

7.8. Possuir relação dos componentes do sistema, onde conste o local e o tipo instalado;

7.9. Possuir sistema de gravação dos diálogos telefônicos, os quais poderão ser verificados posteriormente, num período de até 60 (sessenta) dias;

7.10. É de responsabilidade do CONTRATADO a realização dos serviços de manutenção necessários a garantir o perfeito funcionamento dos equipamentos instalados, bem como o fornecimento de todas as peças e componentes necessários, incluindo baterias, quando couberem, não ensejando custo adicional ao BANCO, além do definido no custo mensal de manutenção;

7.11. Deverão ser realizadas manutenções preventivas nos recursos ao menos 1 vez por semestre;

7.12. Durante toda a vigência do contrato, o contratado será também o responsável pela garantia de todos os seus componentes, mesmo que fabricados, montados ou instalados por terceiros;

7.13. No caso de ocorrerem quaisquer defeitos nos equipamentos, as manutenções corretivas necessárias deverão prover solução no prazo máximo de 24 (vinte e quatro) horas corridas, para as unidades localizadas nas capitais dos estados e respectivas Regiões Metropolitanas, e 48 (quarenta e oito) horas corridas, para as demais unidades;

7.14. Os prazos serão iniciados a contar da data e hora da falha do equipamento registrada em sistema pela supervisão e monitoramento do CONTRATADO ou solicitação efetuada pelo BANCO, por meio de e-mail ou sistema de gestão de demandas do CONTRATADO;

7.15. Para efeito de contagem de tempo, caso o chamado seja feito em finais de semana, feriados nacionais ou em horário fora do expediente comercial (8h às 18h), o prazo para atendimento técnico será iniciado a partir das 8h do dia útil seguinte ao da abertura desse chamado;

7.16. O atendimento deverá ser feito, independente de feriado ou final de semana, salvo disposição em contrário da Unidade, devidamente autorizada pela área de segurança do BANCO. Para esses casos, o tempo de chamado será suspenso;

7.17. A falta de peças no mercado não poderá ser alegada como motivo de força maior e não eximirá o CONTRATADO ao cumprimento dos prazos estabelecidos;

7.18. As manutenções poderão ser executadas por equipe subcontratada do CONTRATADO, desde que supervisionada, local ou remotamente, por funcionário do quadro permanente do CONTRATADO, como forma de garantia de serviços esperados, padronização e responsabilidades direta do CONTRATADO;

7.19. O suporte técnico deverá ser prestado por equipe técnica do CONTRATADO lotada na Direção Geral do Banco do Nordeste, situada em Fortaleza-CE, podendo ser complementada por equipe extrarregional, conforme critério do CONTRATADO;

7.20. O dimensionamento da equipe técnica ficará a cargo do CONTRATADO, bem como todas as obrigações legais, trabalhista, treinamentos e demais necessidades para o pleno desempenho de função de suporte técnico;

7.21. As estações de trabalho (mesa, cadeira, computador e acessórios) serão fornecidas pelo Banco;

7.22. Os profissionais alocados na prestação dos serviços deverão possuir perfil técnico e profissional adequado ao escopo do serviço a ser realizado, devendo ser continuamente treinados, às expensas do CONTRATADO, e avaliados para assegurar o bom desempenho de suas atribuições, além de contribuir para o processo de melhoria contínua, visando a evolução profissional dos mesmos em função das atualizações tecnológicas, que venham a acontecer nesses ambientes, admitindo-se, durante a execução do contrato, a substituição de técnicos por profissionais de experiência equivalente ou superior, com a anuência formal do Banco;

7.23. Os membros das equipes deverão atuar exclusivamente na execução dos serviços contratados durante toda a jornada de trabalho, não sendo admitido o compartilhamento de tempo com outras atividades alheias ao objeto do contrato;

7.24. Os profissionais do CONTRATADO sujeitar-se-ão a todas as normas internas de segurança do Banco, notadamente no que se refere à identificação (uso de crachá), acessos, trânsito e permanência nas instalações do Banco;

7.25. Garantir e manter total e absoluto sigilo sobre as informações manuseadas, conforme consta no Acordo de Responsabilidade para Fornecedores e Parceiros, as quais devem ser utilizadas apenas para a condução das atividades autorizadas, não podendo ter quaisquer outros usos, sob pena de rescisão contratual e medidas cíveis e penais cabíveis;

7.26. Assumir o compromisso de responder perante o Banco, mesmo no caso de ausência ou omissão de fiscalização, indenizando-o por quaisquer atos ou fatos lesivos aos seus interesses, que possam interferir na execução do Contrato, quer sejam eles praticados por empregados, prepostos ou mandatários do CONTRATADO.

8. DEDUÇÕES FINANCEIRAS POR INDISPONIBILIDADE DE SISTEMA

8.1. Após a instalação do sistema havendo paralisação parcial ou total do(s) componente(s) do sistema, no decorrer do mês, serão aplicados descontos diretos em fatura mensal, sem a necessidade de abertura de processo administrativo;

8.2. Até 10 (dez) dias de interrupção, passados os prazos do subitem 7.13, dedução do valor proporcional, em dias, ao tempo em que o(s) equipamento(s) permanecer(em) inoperante(s), aplicável sobre o valor apurado para pagamento dos serviços naquele mês, para aquela Unidade, em que se verificar a ocorrência faltosa, incluindo locação, monitoramento e manutenção;

8.3. Do 10º (décimo) ao 30º (trigésimo) dia de interrupção, a dedução corresponderá ao valor integral apurado para pagamento dos serviços daquele item, naquele mês, para aquela unidade, em que se verificar a ocorrência faltosa, incluindo locação e manutenção;

8.4. A dedução do valor integral persistirá pelos meses subsequentes, caso o problema persista e o item do sistema não retorne ao seu funcionamento pleno, facultado ao BANCO a possibilidade de instaurar Sanções Administrativas.

9. TREINAMENTO DE OPERAÇÃO

9.1. O CONTRATADO deverá ministrar treinamento para equipe da Central de Segurança do BANCO, na cidade de Fortaleza/CE, sobre a operação dos equipamentos e softwares do sistema;

9.2. Na ocasião do treinamento, deverá ser disponibilizado o manual de operação do sistema em via eletrônica e impressa;

9.3. Deverá ser orientado aos usuários dos dispositivos instalados nas agências sobre o funcionamento dos equipamentos e fluxo de operações a ser definido pelo BANCO.

10. DOCUMENTAÇÃO

10.1. Ao final da instalação de cada Agência, o CONTRATADO deverá entregar o projeto *as-built* em formato DWG;

10.2. Todo fornecimento de materiais, equipamentos, instalação, testes e serviços deverão observar rigorosamente as normas técnicas vigentes da ABNT – Associação Brasileira de Normas Técnicas, notadamente a NBR 5410 - Instalações Elétricas de Baixa Tensão.

11. SOFTWARES

11.1. São de responsabilidade do CONTRATADO o fornecimento e a instalação das licenças dos softwares e licenças do sistema integrado, do tipo permanente, sendo de sua completa responsabilidade a realização das instalações e configurações necessárias para o pleno funcionamento e integrações que couberem;

11.2. As atualizações de software deverão ser disponibilizadas durante o período de vigência do contrato, contemplando envio periódico de novas versões do sistema e correção de eventuais falhas e vulnerabilidades do sistema;

11.3. As ações devem ser executadas prioritariamente de forma local em rede interna do BANCO pela equipe de suporte técnico alocada, conforme subitem 7.19;

11.4. Conexões remotas serão tratadas como exceção e casos emergenciais ou urgências, a serem avaliadas criteriosamente pelo BANCO;

11.5. As novas versões do sistema deverão ser instaladas pelo CONTRATADO no prazo de até 60 (sessenta) dias corridos, contado a partir da liberação do fabricante, cujo planejamento será realizado em conjunto com o BANCO;

11.6. Eventuais falhas e vulnerabilidades detectadas no sistema deverão ser corrigidas pelo CONTRATADO no prazo de até 48 (quarenta e oito) horas corridas, contado a partir do chamado do BANCO;

11.7. O CONTRATADO deverá adequar os processos de intervenção aos sistemas, conforme sistemática e ferramentas de versionamento corporativa do BANCO.

12. OBRIGAÇÕES ESPECÍFICAS DO CONTRATADO

12.1. O pessoal técnico do CONTRATADO sujeitar-se-á a todas as normas internas de segurança do BANCO, notadamente no que se refere à identificação (uso de crachá), trânsito e permanência nas instalações do BANCO;

12.2. Cumprir fielmente o Contrato, de modo que os serviços contratados sejam adequados e suficientes para que os equipamentos permaneçam em condições de perfeito e regular funcionamento, cumprindo rigorosamente os prazos estabelecidos;

12.3. O CONTRATADO deverá manter estrutura de coordenação e suporte técnico compatível com a abrangência geográfica das unidades atendidas pelo contrato, incluindo, durante a fase de implantação, coordenação técnica dedicada para interlocução com o BANCO e acompanhamento da execução dos serviços. Adicionalmente, deverá dispor de representação técnica, ponto focal ou coordenação regional nas localidades ou regiões de atuação, dotados de meios adequados de comunicação e gestão, de forma a assegurar o cumprimento dos níveis de serviço estabelecidos, a coordenação das equipes de campo, a padronização dos procedimentos operacionais e o pronto atendimento das demandas do BANCO, devendo comprovar essa condição sempre que solicitado;

12.4. Fornecer, sempre que solicitado pelo BANCO, as especificações dos equipamentos, componentes, acessórios e suprimentos, bem como orientações quanto a procedimentos especiais para operação, ficando ainda, obrigado a fornecer os manuais dos equipamentos no ato da entrega/instalação dos mesmos;

12.5. Coordenar e supervisionar os serviços, através de seus encarregados, sendo que nas manutenções corretivas todo o sistema deverá ser testado, em conjunto com um preposto do BANCO e aferidos/validados pela Área de Segurança do BANCO;

12.6. Atender prontamente às solicitações do BANCO para a realização de serviços extraordinários, informando os dados dos técnicos responsáveis pelo serviço e data de execução do mesmo;

12.7. Fornecer ao BANCO relação nominal das pessoas que efetuarão os serviços de instalação ou manutenção, nela contendo nome, identidade, matrícula, foto e quaisquer outros elementos individuais, indicando os meios para localização de seu preposto junto ao BANCO. Eventuais alterações (exclusão/inclusão de técnicos) verificadas durante a vigência do Contrato deverão ser imediatamente comunicadas ao BANCO;

12.8. Diligenciar para que seus empregados tratem com urbanidade e cortesia os prepostos do BANCO, clientes, visitantes e demais contratados, mantendo-os devidamente uniformizados e portando crachá de identificação, quando em serviço nas dependências do BANCO;

12.9. Reparar prontamente os danos e avarias causados por seus empregados ou prepostos aos bens do BANCO por ocasião das visitas de manutenção ou efetuar a troca do sistema danificado, ficando este autorizado a descontar o valor correspondente dos pagamentos que efetuará ao CONTRATADO;

12.10. Comunicar imediatamente ocorrências que envolvam seus empregados nas dependências do BANCO;

12.11. Dar ciência ao BANCO, imediatamente e por escrito, de qualquer anormalidade que verificar na execução dos serviços;

12.12. Fornecer aos seus técnicos todas as ferramentas e equipamentos necessários à perfeita execução das manutenções ou trocas;

12.13. Assumir o compromisso de responder perante o BANCO, mesmo no caso de ausência ou omissão de fiscalização, indenizando-o por quaisquer atos ou fatos lesivos aos seus interesses, que possam interferir na execução do contrato, quer sejam eles praticados por empregados, prepostos, subempreiteiros, ou mandatários do CONTRATADO. A responsabilidade se estenderá a danos causados a terceiros, devendo a empresa observar as exigências das autoridades competentes e das disposições legais vigentes;

12.14. O CONTRATADO deverá autorizar o BANCO a descontar o valor correspondente aos referidos danos diretamente das faturas pertinentes aos pagamentos que lhe forem devidos, independentemente de quaisquer procedimentos judicial ou extrajudicial;

12.15. Indenizar o BANCO no caso de incidentes, que resulte em prejuízo para o BANCO, desde que fique comprovada a responsabilidade do CONTRATADO, por ineficiência do sistema ou a constatação de defeito não sanado dentro do prazo estipulado em contrato, sem prejuízo das demais cominações aplicáveis. O valor dessa indenização corresponderá aos prejuízos materiais calculados pelo BANCO;

12.16. Os custos eventualmente incorridos pela Unidade do BANCO, sejam com vigilância armada adicional ou quaisquer outros, justificados pela necessidade de recompor a segurança mínima na Unidade, decorrentes de inoperância total ou parcial por mau funcionamento ou defeito de seus acessórios, devidamente comprovada, poderão ser integralmente repassados ao CONTRATADO, caso os prazos de atendimento estabelecidos no subitem não sejam cumpridos.

12.17. Indenizar o BANCO no caso de falha em qualquer um dos sistemas, quando da ocasião de testes da Polícia Federal, referente ao Plano de Segurança, desde que fique comprovada a responsabilidade do CONTRATADO por ineficiência do sistema, omissão no monitoramento do sistema pela equipe de Monitoramento do CONTRATADO ou a constatação de defeito não sanado dentro do prazo estipulado em contrato, sem prejuízo das demais cominações aplicáveis. O valor dessa indenização corresponderá ao valor da multa, em UFIRs, a ser paga pelo BANCO;

12.18. Refazer os serviços julgados pela fiscalização como mal executados, sem ônus para o BANCO;

12.19. Tratar exclusivamente por meio de seu preposto, casos de execução inadequada do serviço ou de outras situações que impliquem a necessidade temporária de alteração na forma em que o serviço deva ser executado;

12.20. Em sendo necessário efetuar consertos de maior extensão / complexidade, sendo indispensável a retirada de componentes ou do equipamento para reparo fora das dependências do BANCO, o CONTRATADO deverá disponibilizar e instalar equipamento compatível, em substituição ao defeituoso, sem qualquer custo ao BANCO, permanecendo o equipamento em uso até a devolução e instalação do equipamento locado, devidamente reparado.